		_
Clarke	Jackson (IL)	Peterson (MN)
Clay	Jackson-Lee	Pomeroy
Cleaver	(TX)	Price (NC)
Clyburn	Jefferson	Rahall
Cohen	Johnson (GA)	Rangel
Conyers	Johnson, E. B.	Reyes
Cooper	Jones (OH)	Richardson
Costa	Kagen	Rodriguez
Costello	Kanjorski	Ross
Courtney	Kaptur	Rothman
Cramer	Kennedy	Roybal-Allard
Crowley	Kildee	Ryan (OH)
Cuellar	Kilpatrick	Salazar
Cummings	Kind	Sánchez, Linda
Davis (AL)	Klein (FL)	Т.
Davis (CA)	Kucinich	Sanchez, Lorett
Davis (IL)	Lampson	Sarbanes
DeFazio	Larsen (WA)	Schakowsky
DeGette	Larson (CT)	Schiff
Delahunt	Lee	Schwartz
DeLauro	Levin	Scott (VA)
Dicks	Lewis (GA)	Serrano
Dingell Doggott	Lipinski Loebsack	Sestak
Doggett Donnelly	Lofgren, Zoe	Shea-Porter
Donnerry Doyle	Lorgren, Zoe Lowey	Sherman
Edwards (MD)	Lynch	Shuler
Edwards (TX)	Mahoney (FL)	Sires
Ellison	Maloney (NY)	Skelton
Ellsworth	Markey	Slaughter
Emanuel	Marshall	Smith (WA)
Engel	Matheson	Snyder
Eshoo	Matsui	Solis
Etheridge	McCarthy (NY)	Space
Farr	McCollum (MN)	Speier
Fattah	McDermott	Spratt
Filner	McGovern	Stupak
Foster	McIntyre	Sutton
Frank (MA)	McNerney	Tanner
Giffords	McNulty	Tauscher
Gillibrand	Meek (FL)	Taylor
Gonzalez	Melancon	Thompson (CA)
Gordon	Michaud	Thompson (MS)
Green, Al	Miller (NC)	Tierney
Green, Gene	Miller, George	Tsongas
Grijalva	Mitchell	Udall (CO)
Gutierrez	Mollohan	Udall (NM)
Hall (NY)	Moore (KS)	Van Hollen
Hare	Moore (WI)	Velázquez
Harman	Moran (VA)	Walz (MN)
Hastings (FL)	Murphy (CT)	Wasserman
Herseth Sandlin	Murphy, Patrick	Schultz
Higgins	Murtha	Waters
Hinchey	Nadler	Watson
Hinojosa Hirono	Napolitano	Watt
Hodes	Neal (MA) Obey	Waxman
Holden		Weiner
Holt	Olver Ortiz	Welch (VT)
Honda	Pallone	Wexler
Hooley	Pascrell	Wilson (OH)
Hoyer Hoyer	Pastor	Woolsey
Inslee	Payne	Wu
Israel	Perlmutter	Yarmuth
FDT 01.CT	1 CHIHADOEL	1 ai iiiuuli

NOES-185

	NOES-185	
Aderholt	Coble	Gingrey
Akin	Cole (OK)	Goode
Alexander	Conaway	Goodlatte
Bachmann	Crenshaw	Graves
Bachus	Cubin	Hall (TX)
Barrett (SC)	Culberson	Hastings (WA)
Barton (TX)	Davis (KY)	Hayes
Biggert	Davis, David	Heller
Bilirakis	Davis, Tom	Hensarling
Bishop (UT)	Deal (GA)	Herger
Blackburn	Dent	Hill
Blunt	Diaz-Balart, L.	Hobson
Boehner	Diaz-Balart, M.	Hoekstra
Bonner	Doolittle	Hulshof
Bono Mack	Drake	Hunter
Boozman	Dreier	Inglis (SC)
Boustany	Duncan	Issa
Brady (TX)	Ehlers	Johnson (IL)
Broun (GA)	Emerson	Johnson, Sam
Brown (SC)	English (PA)	Jordan
Buchanan	Everett	Keller
Burgess	Fallin	King (IA)
Burton (IN)	Feeney	King (NY)
Buyer	Flake	Kingston
Calvert	Forbes	Kirk
Camp (MI)	Fortenberry	Kline (MN)
Campbell (CA)	Fossella	Knollenberg
Cantor	Foxx	Kuhl (NY)
Capito	Franks (AZ)	LaHood
Carter	Frelinghuysen	Lamborn
Castle	Gallegly	Latham
Cazayoux	Garrett (NJ)	LaTourette
Chabot	Gerlach	Latta

Lewis (CA)	Pence	Shadegg
Lewis (KY)	Petri	Shays
Linder	Pickering	Shimkus
LoBiondo	Pitts	Shuster
Lucas	Platts	Simpson
Lungren, Daniel	Poe	Smith (NE)
E.	Porter	Smith (NJ)
Mack	Price (GA)	Smith (TX)
Manzullo	Pryce (OH)	Souder
Marchant	Putnam	Stearns
McCarthy (CA)	Radanovich	Sullivan
McCaul (TX)	Ramstad	Tancredo
McCotter	Regula	
McCrery	Rehberg	Terry
McHenry	Reichert	Thornberry
McHugh	Renzi	Tiberi
McKeon	Rogers (AL)	Turner
McMorris	Rogers (KY)	Upton
Rodgers	Rogers (MI)	Walberg
Mica	Rohrabacher	Walden (OR)
Miller (FL)	Ros-Lehtinen	Walsh (NY)
Miller (MI)	Roskam	Wamp
Miller, Gary	Royce	Weldon (FL)
Moran (KS)	Ryan (WI)	Westmoreland
Murphy, Tim	Sali	Whitfield (KY)
Musgrave	Saxton	Wilson (SC)
Myrick	Scalise	Wittman (VA)
Neugebauer	Schmidt	Wolf
Nunes	Sensenbrenner	
Pearce	Sessions	Young (FL)

NOT VOTING-26

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE The SPEAKER pro tempore (during the vote). There are 2 minutes remaining on this vote.

□ 1045

So the resolution was agreed to.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

Stated for:

Mr. RUPPERSBERGER. Madam Speaker, on rollcall No. 436, I was meeting with constituents in my district office. Had I been present, I would have voted "aye."

Mr. VISCLOSKY. Madam Speaker, had I been present for rollcall 436. H. Res. 1276. on agreeing to the resolution providing for the consideration of H.R. 5876, the Stop Child Abuse in Residential Programs for Teens Act of 2008, I would have voted "aye."

FISA AMENDMENTS ACT OF 2008

Mr. CONYERS. Madam Speaker, pursuant to House Resolution 1285, I call up the bill (H.R. 6304) to amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes, and ask for its immediate consideration in the House.

The Clerk read the title of the bill. The text of the bill is as follows:

H.R. 6304

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008" or the "FISA Amendments Act of 2008"

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE

Sec. 101. Additional procedures regarding certain persons outside the United States.

Sec. 102. Statement of exclusive means by which electronic surveillance and interception of certain communications may be conducted.

Sec. 103. Submittal to Congress of certain court orders under the Foreign Intelligence Surveillance Act of 1978

Sec. 104. Applications for court orders.

Sec. 105. Issuance of an order.

Sec. 106. Use of information.

Sec. 107. Amendments for physical searches. Sec. 108. Amendments for emergency pen registers and trap and trace devices.

Sec. 109. Foreign Intelligence Surveillance Court.

Sec. 110. Weapons of mass destruction.

TITLE II—PROTECTIONS FOR ELEC-TRONIC COMMUNICATION SERVICE PROVIDERS

Sec. 201. Procedures for implementing statutory defenses under the Foreign Intelligence Surveillance Act of 1978.

Sec. 202. Technical amendments.

TITLE III—REVIEW OF PREVIOUS ACTIONS

Sec. 301. Review of previous actions. TITLE IV—OTHER PROVISIONS

Sec. 401. Severability.

Sec. 402. Effective date.

Sec. 403. Repeals.

Sec. 404. Transition procedures.

TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE

SEC. 101. ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES.

(a) IN GENERAL.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) by striking title VII; and

(2) by adding at the end the following:

"TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUT-SIDE THE UNITED STATES

"SEC. 701. DEFINITIONS.

"(a) IN GENERAL.—The terms 'agent of a foreign power', 'Attorney General', 'contents', 'electronic surveillance', 'foreign intelligence information', 'foreign power'. 'person', 'United States', and 'United States person' have the meanings given such terms in section 101, except as specifically provided in this title.

"(b) Additional Definitions —

"(1) CONGRESSIONAL INTELLIGENCE COMMIT-TEES.—The term 'congressional intelligence committees' means-

"(A) the Select Committee on Intelligence of the Senate; and

"(B) the Permanent Select Committee on Intelligence of the House of Representatives.

"(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT; COURT.-The terms 'Foreign Intelligence Surveillance Court' and 'Court' mean the court established under section 103(a).

"(3) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW; COURT OF REVIEW.-The terms 'Foreign Intelligence Surveillance Court of Review' and 'Court of Review' mean the court established under section 103(b).

"(4) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term 'electronic communication service provider' means-

"(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

- "(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;
- "(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;
- "(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or
- "(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).
- "(5) INTELLIGENCE COMMUNITY.—The term intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

"SEC. 702. PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS.

- "(a) AUTHORIZATION.—Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.
- "(b) LIMITATIONS.—An acquisition authorized under subsection (a)—
- "(1) may not intentionally target any person known at the time of acquisition to be located in the United States;
- "(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States:
- "(3) may not intentionally target a United States person reasonably believed to be located outside the United States;
- "(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States: and
- "(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.
- "(c) CONDUCT OF ACQUISITION.—
- "(1) IN GENERAL.—An acquisition authorized under subsection (a) shall be conducted only in accordance with—
- "(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and
- "(B) upon submission of a certification in accordance with subsection (g), such certification.
- "(2) DETERMINATION.—A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (i)(3) prior to the implementation of such authorization.
- "(3) TIMING OF DETERMINATION.—The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)—
- "(A) before the submission of a certification in accordance with subsection (g); or
- "(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) of such certification is pending.

- "(4) Construction.—Nothing in title I shall be construed to require an application for a court order under such title for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.
 - "(d) Targeting Procedures.—
- "(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to—
- "(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States: and
- "(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.
- "(2) JUDICIAL REVIEW.—The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).
 - "(e) MINIMIZATION PROCEDURES.—
- "(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, for acquisitions authorized under subsection (a).
- "(2) JUDICIAL REVIEW.—The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).
- "(f) GUIDELINES FOR COMPLIANCE WITH LIM-
- "(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure—
- ``(A) compliance with the limitations in subsection (b); and
- "(B) that an application for a court order is filed as required by this Act.
- "(2) SUBMISSION OF GUIDELINES.—The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to—
- "(A) the congressional intelligence committees;
- "(B) the Committees on the Judiciary of the Senate and the House of Representatives; and
- $\mbox{``(C)}$ the Foreign Intelligence Surveillance Court.
- "(g) CERTIFICATION.—
- "(1) IN GENERAL.—
- "(A) REQUIREMENT.—Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.
- "(B) EXCEPTION.—If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for such authorization as soon as practicable but in no event later than 7 days after such determination is made.
- ``(2) REQUIREMENTS.—A certification made under this subsection shall—
 - "(A) attest that-
- "(i) there are procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intel-

- ligence Surveillance Court that are reasonably designed to—
- "(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and
- "(II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;
- "(ii) the minimization procedures to be used with respect to such acquisition—
- "(I) meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and
- "(II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court;
- "(iii) guidelines have been adopted in accordance with subsection (f) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this Act;
- "(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States:
- ``(v) a significant purpose of the acquisition is to obtain foreign intelligence information;
- "(vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and
- "(vii) the acquisition complies with the limitations in subsection (b):
- "(B) include the procedures adopted in accordance with subsections (d) and (e);
- "(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is—
- "(i) appointed by the President, by and with the advice and consent of the Senate: or
- "(ii) the head of an element of the intelligence community;
 - "(D) include-
- "(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or
- "(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and
- "(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.
- "(3) CHANGE IN EFFECTIVE DATE.—The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (i)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).
- "(4) LIMITATION.—A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.
- "(5) MAINTENANCE OF CERTIFICATION.—The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.
- "(6) REVIEW.—A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (i).
- "(h) DIRECTIVES AND JUDICIAL REVIEW OF DIRECTIVES.—
- "(1) AUTHORITY.—With respect to an acquisition authorized under subsection (a), the

Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—

- "(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and
- "(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.
- "(2) COMPENSATION.—The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).
- "(3) RELEASE FROM LIABILITY.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).
- "(4) CHALLENGING OF DIRECTIVES.-
- "(A) AUTHORITY TO CHALLENGE.—An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.
- "(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) not later than 24 hours after the filing of such petition.
- "(C) STANDARDS FOR REVIEW.—A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.
- "(D) PROCEDURES FOR INITIAL REVIEW.—A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it. Upon making a determination under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.
- "(E) PROCEDURES FOR PLENARY REVIEW.—If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.
- "(F) CONTINUED EFFECT.—Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

- "(G) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.
 - ``(5) Enforcement of directives.—
- "(A) ORDER TO COMPEL.—If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.
- "(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) not later than 24 hours after the filing of such petition.
- "(C) PROCEDURES FOR REVIEW.—A judge considering a petition filed under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.
- "(D) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.
- "(E) PROCESS.—Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.
- "(6) APPEAL.-
- "(A) APPEAL TO THE COURT OF REVIEW.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.
- "(B) CERTIORARI TO THE SUPREME COURT.— The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.
- "(i) JUDICIAL REVIEW OF CERTIFICATIONS AND PROCEDURES —
- "(1) IN GENERAL.—
- "(A) REVIEW BY THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e), and amendments to such certification or such procedures.
- "(B) TIME PERIOD FOR REVIEW.—The Court shall review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.
- "(C) AMENDMENTS.—The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting and minimization procedures adopted in accordance with subsections (d) and (e) as nec-

- essary at any time, including if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court's review of such amended certification or amended procedures.
- ``(2) REVIEW.—The Court shall review the following:
- "(A) CERTIFICATION.—A certification submitted in accordance with subsection (g) to determine whether the certification contains all the required elements.
- "(B) TARGETING PROCEDURES.—The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to—
- "(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and
- "(ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.
- "(C) MINIMIZATION PROCEDURES.—The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 101(h) or section 301(4), as appropriate.
 - "(3) ORDERS.-
- "(A) APPROVAL.—If the Court finds that a certification submitted in accordance with subsection (g) contains all the required elements and that the targeting and minimization procedures adopted in accordance with subsections (d) and (e) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.
- "(B) CORRECTION OF DEFICIENCIES.—If the Court finds that a certification submitted in accordance with subsection (g) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order—
- "(i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or
- "(ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.
- "(C) REQUIREMENT FOR WRITTEN STATE-MENT.—In support of an order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.
 - "(4) APPEAL.-
- "(A) APPEAL TO THE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming,

reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

''(B) CONTINUATION OF ACQUISITION PENDING REHEARING OR APPEAL.—Any acquisition affected by an order under paragraph (3)(B) may continue—

"(i) during the pendency of any rehearing of the order by the Court en banc; and

"(ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

"(C) IMPLEMENTATION PENDING APPEAL.— Not later than 60 days after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

"(D) CERTIORARI TO THE SUPREME COURT.— The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

"(5) SCHEDULE.-

"(A) REAUTHORIZATION OF AUTHORIZATIONS IN EFFECT.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (g) and the procedures adopted in accordance with subsections (d) and (e) at least 30 days prior to the expiration of such authorization.

"(B) REAUTHORIZATION OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues an order with respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

"(j) JUDICIAL PROCEEDINGS.—

"(1) EXPEDITED JUDICIAL PROCEEDINGS.—Judicial proceedings under this section shall be conducted as expeditiously as possible.

"(2) TIME LIMITS.—A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

"(k) MAINTENANCE AND SECURITY O RECORDS AND PROCEEDINGS.—

"(1) STANDARDS.—The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

"(2) FILING AND REVIEW.—All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review ex parte and in camera any Govern-

ment submission, or portions of a submission, which may include classified information.

"(3) RETENTION OF RECORDS.—The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued.

"(1) Assessments and Reviews.—

"(1) SEMIANNUAL ASSESSMENT.—Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f) and shall submit each assessment to—

"(A) the Foreign Intelligence Surveillance Court: and

"(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

"(i) the congressional intelligence committees: and

"(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

"(2) AGENCY ASSESSMENT.—The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General—

"(A) are authorized to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f);

"(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United Statesperson identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

"(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

"(D) shall provide each such review to—

"(i) the Attorney General;

"(ii) the Director of National Intelligence; and

"(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

"(I) the congressional intelligence committees; and

"(II) the Committees on the Judiciary of the House of Representatives and the Senate. "(3) ANNUAL REVIEW —

"(A) REQUIREMENT TO CONDUCT.—The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)—

"(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;

"(ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;

"(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

"(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.

"(B) USE OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).

"(C) PROVISION OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to—

``(i) the Foreign Intelligence Surveillance Court:

"(ii) the Attorney General;

"(iii) the Director of National Intelligence;

"(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

"(I) the congressional intelligence committees; and

"(II) the Committees on the Judiciary of the House of Representatives and the Senate.

"SEC. 703. CERTAIN ACQUISITIONS INSIDE THE UNITED STATES TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES.

"(a) JURISDICTION OF THE FOREIGN INTEL-LIGENCE SURVEILLANCE COURT.—

"(1) IN GENERAL.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires an order under this Act, and such acquisition is conducted within the United States.

(2) LIMITATION.—If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States while an order issued pursuant to subsection (c) is in effect. Nothing in this section shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.

"(b) APPLICATION.—

"(1) IN GENERAL.—Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General's finding

- that it satisfies the criteria and requirements of such application, as set forth in this section, and shall include—
- "(A) the identity of the Federal officer making the application;
- "(B) the identity, if known, or a description of the United States person who is the target of the acquisition;
- "(C) a statement of the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target of the acquisition is—
- "(i) a person reasonably believed to be located outside the United States; and
- "(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;
- "(D) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate;
- "(E) a description of the nature of the information sought and the type of communications or activities to be subjected to acquisition;
- "(F) a certification made by the Attorney General or an official specified in section 104(a)(6) that—
- "(i) the certifying official deems the information sought to be foreign intelligence information:
- "(ii) a significant purpose of the acquisition is to obtain foreign intelligence information;
- "(iii) such information cannot reasonably be obtained by normal investigative techniques:
- "(iv) designates the type of foreign intelligence information being sought according to the categories described in section 101(e); and
- ``(v) includes a statement of the basis for the certification that—
- "(I) the information sought is the type of foreign intelligence information designated; and
- "(II) such information cannot reasonably be obtained by normal investigative techniques;
- "(G) a summary statement of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition;
- "(H) the identity of any electronic communication service provider necessary to effect the acquisition, provided that the application is not required to identify the specific facilities, places, premises, or property at which the acquisition authorized under this section will be directed or conducted;
- "(I) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application; and
- "(J) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application.
- "(2) OTHER REQUIREMENTS OF THE ATTORNEY GENERAL.—The Attorney General may require any other affidavit or certification from any other officer in connection with the application.
- "(3) OTHER REQUIREMENTS OF THE JUDGE.— The judge may require the applicant to furnish such other information as may be necessary to make the findings required by subsection (c)(1).
- "(c) ORDER.—
- "(1) FINDINGS.—Upon an application made pursuant to subsection (b), the Foreign Intelligence Surveillance Court shall enter an exparte order as requested or as modified by the Court approving the acquisition if the Court finds that—

- "(A) the application has been made by a Federal officer and approved by the Attorney General:
- "(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—
- "(i) a person reasonably believed to be located outside the United States; and
- "(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;
- "(C) the proposed minimization procedures meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and
- "(D) the application that has been filed contains all statements and certifications required by subsection (b) and the certification or certifications are not clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3).
- "(2) PROBABLE CAUSE.—In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target. No United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.
 - "(3) REVIEW .-
- "(A) LIMITATION ON REVIEW.—Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1).
- "(B) REVIEW OF PROBABLE CAUSE.—If the judge determines that the facts submitted under subsection (b) are insufficient to establish probable cause under paragraph (1)(B), the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).
- "(C) REVIEW OF MINIMIZATION PROCE-DURES.—If the judge determines that the proposed minimization procedures referred to in paragraph (1)(C) do not meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).
- "(D) REVIEW OF CERTIFICATION.—If the judge determines that an application pursuant to subsection (b) does not contain all of the required elements, or that the certification or certifications are clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3), the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).
- "(4) SPECIFICATIONS.—An order approving an acquisition under this subsection shall specify—
- "(A) the identity, if known, or a description of the United States person who is the target of the acquisition identified or described in the application pursuant to subsection (b)(1)(B):
- "(B) if provided in the application pursuant to subsection (b)(1)(H), the nature and location of each of the facilities or places at which the acquisition will be directed;

- "(C) the nature of the information sought to be acquired and the type of communications or activities to be subjected to acquisition:
- "(D) a summary of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition; and
- "(E) the period of time during which the acquisition is approved.
- ''(5) DIRECTIVES.—An order approving an acquisition under this subsection shall direct—
- "(A) that the minimization procedures referred to in paragraph (1)(C), as approved or modified by the Court, be followed;
- "(B) if applicable, an electronic communication service provider to provide to the Government forthwith all information, facilities, or assistance necessary to accomplish the acquisition authorized under such order in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition:
- "(C) if applicable, an electronic communication service provider to maintain under security procedures approved by the Attorney General any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain; and
- "(D) if applicable, that the Government compensate, at the prevailing rate, such electronic communication service provider for providing such information, facilities, or assistance.
- "(6) DURATION.—An order approved under this subsection shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b)
- "(7) COMPLIANCE.—At or prior to the end of the period of time for which an acquisition is approved by an order or extension under this section, the judge may assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was acquired, retained or disseminated
 - "(d) EMERGENCY AUTHORIZATION.—
- "(1) AUTHORITY FOR EMERGENCY AUTHORIZATION.—Notwithstanding any other provision of this Act, if the Attorney General reasonably determines that—
- "(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order authorizing such acquisition can with due diligence be obtained, and
- "(B) the factual basis for issuance of an order under this subsection to approve such acquisition exists,
- the Attorney General may authorize such acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General, or a designee of the Attorney General, at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this section is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.
- "(2) MINIMIZATION PROCEDURES.—If the Attorney General authorizes an acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (c)(1)(C) for the issuance of a judicial order be followed.
- "(3) TERMINATION OF EMERGENCY AUTHORIZATION.—In the absence of a judicial order

approving an acquisition under paragraph (1), such acquisition shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

"(4) USE OF INFORMATION.—If an application for approval submitted pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order is issued approving the acquisition, no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing. or other proceeding in or before any court. grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

"(e) RELEASE FROM LIABILITY.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with an order or request for emergency assistance issued pursuant to subsection (c) or (d), respectively.

"(f) APPEAL.-

"(1) APPEAL TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order issued pursuant to subsection (c). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.

"(2) CERTIORARI TO THE SUPREME COURT.— The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under paragraph (1). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

"(g) CONSTRUCTION.—Except as provided in this section, nothing in this Act shall be construed to require an application for a court order for an acquisition that is targeted in accordance with this section at a United States person reasonably believed to be located outside the United States.

"SEC. 704. OTHER ACQUISITIONS TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES.

"(a) JURISDICTION AND SCOPE.

"(1) JURISDICTION.—The Foreign Intelligence Surveillance Court shall have jurisdiction to enter an order pursuant to subsection (c).

"(2) Scope.—No element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes, unless a judge of the Foreign Intelligence Surveillance Court has entered an order with respect to such targeted United States person or the Attorney General has authorized an emergency acquisition pursuant to subsection (c) or (d), respectively, or any other provision of this Act.

"(3) LIMITATIONS.—

"(A) MOVING OR MISIDENTIFIED TARGETS.—If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States during the effective period of such order.

"(B) APPLICABILITY.—If an acquisition for foreign intelligence purposes is to be conducted inside the United States and could be authorized under section 703, the acquisition may only be conducted if authorized under section 703 or in accordance with another provision of this Act other than this section.

"(C) CONSTRUCTION.—Nothing in this paragraph shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.

"(b) APPLICATION.—Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements of such application as set forth in this section and shall include—

"(1) the identity of the Federal officer making the application:

"(2) the identity, if known, or a description of the specific United States person who is the target of the acquisition:

"(3) a statement of the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target of the acquisition is—

"(A) a person reasonably believed to be located outside the United States; and

"(B) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

"(4) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate;

"(5) a certification made by the Attorney General, an official specified in section 104(a)(6), or the head of an element of the intelligence community that—

"(A) the certifying official deems the information sought to be foreign intelligence information; and

"(B) a significant purpose of the acquisition is to obtain foreign intelligence information:

"(6) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application; and

"(7) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application.

"(c) Order.—

"(1) FINDINGS.—Upon an application made pursuant to subsection (b), the Foreign Intelligence Surveillance Court shall enter an ex parte order as requested or as modified by the Court if the Court finds that—

"(A) the application has been made by a Federal officer and approved by the Attorney General:

"(B) on the basis of the facts submitted by the applicant, for the United States person

who is the target of the acquisition, there is probable cause to believe that the target is—

"(i) a person reasonably believed to be located outside the United States; and

"(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power:

"(C) the proposed minimization procedures, with respect to their dissemination provisions, meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

"(D) the application that has been filed contains all statements and certifications required by subsection (b) and the certification provided under subsection (b)(5) is not clearly erroneous on the basis of the information furnished under subsection (b).

"(2) PROBABLE CAUSE.—In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target. No United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

"(3) REVIEW -

"(A) LIMITATIONS ON REVIEW.—Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1). The judge shall not have jurisdiction to review the means by which an acquisition under this section may be conducted.

"(B) REVIEW OF PROBABLE CAUSE.—If the judge determines that the facts submitted under subsection (b) are insufficient to establish probable cause to issue an order under this subsection, the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

"(C) REVIEW OF MINIMIZATION PROCE-DURES.—If the judge determines that the minimization procedures applicable to dissemination of information obtained through an acquisition under this subsection do not meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

"(D) SCOPE OF REVIEW OF CERTIFICATION.—If the judge determines that an application under subsection (b) does not contain all the required elements, or that the certification provided under subsection (b)(5) is clearly erroneous on the basis of the information furnished under subsection (b), the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

"(4) DURATION.—An order under this paragraph shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).

(5) COMPLIANCE.—At or prior to the end of the period of time for which an order or extension is granted under this section, the judge may assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was disseminated, provided that the

judge may not inquire into the circumstances relating to the conduct of the acquisition.

- "(d) EMERGENCY AUTHORIZATION.—
- "(1) AUTHORITY FOR EMERGENCY AUTHORIZATION.—Notwithstanding any other provision of this section, if the Attorney General reasonably determines that—
- "(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order under that subsection can, with due diligence, be obtained, and
- "(B) the factual basis for the issuance of an order under this section exists,
- the Attorney General may authorize the emergency acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General or a designee of the Attorney General at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this section is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.
- "(2) MINIMIZATION PROCEDURES.—If the Attorney General authorizes an emergency acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (c)(1)(C) be followed
- "(3) TERMINATION OF EMERGENCY AUTHOR-IZATION.—In the absence of an order under subsection (c), an emergency acquisition under paragraph (1) shall terminate when the information sought is obtained, if the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.
- "(4) USE OF INFORMATION.—If an application submitted to the Court pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order with respect to the target of the acquisition is issued under subsection (c), no information obtained or evidence derived from acquisition. except under cumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.
- "(e) APPEAL.—
- "(1) APPEAL TO THE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order issued pursuant to subsection (c). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.
- "(2) CERTIORARI TO THE SUPREME COURT.— The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under paragraph (1). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision."

"SEC. 705. JOINT APPLICATIONS AND CONCURRENT AUTHORIZATIONS.

- "(a) JOINT APPLICATIONS AND ORDERS.—If an acquisition targeting a United States person under section 703 or 704 is proposed to be conducted both inside and outside the United States, a judge having jurisdiction under section 703(a)(1) or 704(a)(1) may issue simultaneously, upon the request of the Government in a joint application complying with the requirements of sections 703(b) and 704(b), orders under sections 703(c) and 704(c), as appropriate.
- "(b) CONCURRENT AUTHORIZATION.—If an order authorizing electronic surveillance or physical search has been obtained under section 105 or 304, the Attorney General may authorize, for the effective period of that order, without an order under section 703 or 704, the targeting of that United States person for the purpose of acquiring foreign intelligence information while such person is reasonably believed to be located outside the United States.

"SEC. 706. USE OF INFORMATION ACQUIRED UNDER TITLE VII.

- "(a) Information Acquired Under Section 702.—Information acquired from an acquisition conducted under section 702 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106, except for the purposes of subsection (j) of such section.
- "(b) Information Acquired Under Section 703.—Information acquired from an acquisition conducted under section 703 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106.

"SEC. 707. CONGRESSIONAL OVERSIGHT.

- "(a) SEMIANNUAL REPORT.—Not less frequently than once every 6 months, the Attorney General shall fully inform, in a manner consistent with national security, the congressional intelligence committees and the Committees on the Judiciary of the Senate and the House of Representatives, consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution, concerning the implementation of this title.
- "(b) CONTENT.—Each report under subsection (a) shall include—
- "(1) with respect to section 702—
- "(A) any certifications submitted in accordance with section 702(g) during the reporting period;
- "(B) with respect to each determination under section 702(c)(2), the reasons for exercising the authority under such section;
- "(C) any directives issued under section 702(h) during the reporting period;
- "(D) a description of the judicial review during the reporting period of such certifications and targeting and minimization procedures adopted in accordance with subsections (d) and (e) of section 702 and utilized with respect to an acquisition under such section, including a copy of an order or pleading in connection with such review that contains a significant legal interpretation of the provisions of section 702;
- ``(E) any actions taken to challenge or enforce a directive under paragraph (4) or (5) of section 702(h);
- "(F) any compliance reviews conducted by the Attorney General or the Director of National Intelligence of acquisitions authorized under section 702(a);
- "(G) a description of any incidents of non-compliance—
- "(i) with a directive issued by the Attorney General and the Director of National Intelligence under section 702(h), including incidents of noncompliance by a specified person to whom the Attorney General and Director

- of National Intelligence issued a directive under section 702(h); and
- "(ii) by an element of the intelligence community with procedures and guidelines adopted in accordance with subsections (d), (e), and (f) of section 702; and
- "(H) any procedures implementing section 702:
 - "(2) with respect to section 703-
- "(A) the total number of applications made for orders under section 703(b);
 - "(B) the total number of such orders-
 - "(i) granted;
 - "(ii) modified; and
 - "(iii) denied; and
- "(C) the total number of emergency acquisitions authorized by the Attorney General under section 703(d) and the total number of subsequent orders approving or denying such acquisitions; and
 - "(3) with respect to section 704—
- "(A) the total number of applications made for orders under section 704(b);
 - "(B) the total number of such orders—
 - "(i) granted;
 - "(ii) modified; and
 - "(iii) denied; and
- "(C) the total number of emergency acquisitions authorized by the Attorney General under section 704(d) and the total number of subsequent orders approving or denying such applications.

"SEC. 708. SAVINGS PROVISION.

- "Nothing in this title shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.".
- (b) Table of Contents.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—
- (1) by striking the item relating to title VII:
- (2) by striking the item relating to section 701; and
- (3) by adding at the end the following:
- "TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES
- "Sec. 701. Definitions.
- "Sec. 702. Procedures for targeting certain persons outside the United States other than United States persons.
- "Sec. 703. Certain acquisitions inside the United States targeting United States persons outside the United States.
- "Sec. 704. Other acquisitions targeting United States persons outside the United States.
- "Sec. 705. Joint applications and concurrent authorizations.
- "Sec. 706. Use of information acquired under title VII.
- "Sec. 707. Congressional oversight.
- "Sec. 708. Savings provision.".
- (c) Technical and Conforming Amendments.—
- (1) TITLE 18, UNITED STATES CODE.—Section 2511(2)(a)(ii)(A) of title 18, United States Code, is amended by inserting "or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978" after "assistance".
- (2) Foreign intelligence surveillance act of 1978.—Section 601(a)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(a)(1)) is amended—
- (A) in subparagraph (C), by striking "and"; and
- (B) by adding at the end the following new subparagraphs:
 - "(E) acquisitions under section 703; and
 - "(F) acquisitions under section 704;".

SEC. 102. STATEMENT OF EXCLUSIVE MEANS BY WHICH ELECTRONIC SURVEILLANCE AND INTERCEPTION OF CERTAIN COMMUNICATIONS MAY BE CON-

(a) STATEMENT OF EXCLUSIVE MEANS.-Title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by adding at the end the following new section:

"STATEMENT OF EXCLUSIVE MEANS BY WHICH ELECTRONIC SURVEILLANCE AND INTERCEP-TION OF CERTAIN COMMUNICATIONS MAY BE CONDUCTED

"SEC. 112. (a) Except as provided in subsection (b), the procedures of chapters 119. 121, and 206 of title 18. United States Code. and this Act shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.

(b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this Act or chapters 119, 121, or 206 of title 18, United States Code, shall constitute an additional exclusive means for the purpose of subsection (a).

(b) Offense.—Section 109(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1809(a)) is amended by striking "authorized by statute" each place it appears and inserting "authorized by this Act, chapter 119, 121, or 206 of title 18, United States Code, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 112."; and

(c) Conforming Amendments —

(1) TITLE 18, UNITED STATES CODE.—Section 2511(2)(a) of title 18, United States Code, is amended by adding at the end the following:

'(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met."; and

(2) Table of contents.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after the item relating to section 111, the following new item:

"Sec. 112. Statement of exclusive means by which electronic surveillance and interception of certain communications may be conducted."

SEC. 103. SUBMITTAL TO CONGRESS OF CERTAIN COURT ORDERS UNDER THE FOR-EIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) INCLUSION OF CERTAIN ORDERS IN SEMI-ANNUAL REPORTS OF ATTORNEY GENERAL.-Subsection (a)(5) of section 601 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871) is amended by striking "(not including orders)" and inserting ", orders,

(b) REPORTS BY ATTORNEY GENERAL ON CER-TAIN OTHER ORDERS.—Such section 601 is further amended by adding at the end the fol-

(c) Submissions to Congress.—The Attorney General shall submit to the committees of Congress referred to in subsection (a)-

'(1) a copy of any decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review that includes significant construction or interpretation of any provision of this Act, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, not later than 45 days after such decision, order, or opinion is issued; and

"(2) a copy of each such decision, order, or opinion, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, that was issued during the 5-year period ending on the date of the enactment of the FISA Amendments Act of 2008 and not previously submitted in a report under subsection (a).

'(d) PROTECTION OF NATIONAL SECURITY. The Attorney General, in consultation with the Director of National Intelligence, may authorize redactions of materials described in subsection (c) that are provided to the committees of Congress referred to in subsection (a), if such redactions are necessary to protect the national security of the United States and are limited to sensitive sources and methods information or the identities of targets."

(c) DEFINITIONS.—Such section 601, as amended by subsections (a) and (b), is further amended by adding at the end the following:

"(e) DEFINITIONS.—In this section:

"(1) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term 'Foreign Intelligence Surveillance Court' means the court established under section 103(a).

(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The term 'Foreign Intelligence Surveillance Court of Review' means the court established under section 103(b).". SEC. 104. APPLICATIONS FOR COURT ORDERS.

Section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804) is amended-

(1) in subsection (a)—

(A) by striking paragraphs (2) and (11);

by redesignating paragraphs through (10) as paragraphs (2) through (9), respectively:

(C) in paragraph (5), as redesignated by subparagraph (B) of this paragraph, by striking "detailed":

(D) in paragraph (6), as redesignated by subparagraph (B) of this paragraph, in the matter preceding subparagraph (A)

(i) by striking "Affairs or" and inserting 'Affairs,''; and

(ii) by striking "Senate—" and inserting Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—'

(E) in paragraph (7), as redesignated by subparagraph (B) of this paragraph, by striking "statement of" and inserting "summary statement of";

(F) in paragraph (8), as redesignated by subparagraph (B) of this paragraph, by adding "and" at the end; and

(G) in paragraph (9), as redesignated by subparagraph (B) of this paragraph, by strik-"; and" and inserting a period;

(2) by striking subsection (b);

by redesignating subsections (c) through (e) as subsections (b) through (d), respectively; and

(4) in paragraph (1)(A) of subsection (d), as redesignated by paragraph (3) of this subsection, by striking "or the Director of National Intelligence" and inserting "the Director of National Intelligence, or the Director of the Central Intelligence Agency".

SEC. 105. ISSUANCE OF AN ORDER.

(a) IN GENERAL.—Section 105 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805) is amended-

(1) in subsection (a)-

(A) by striking paragraph (1); and

(B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively:

(2) in subsection (b), by striking "(a)(3)" and inserting "(a)(2)";

(3) in subsection (c)(1)-

(A) in subparagraph (D), by adding "and" at the end;

(B) in subparagraph (E), by striking "; and" and inserting a period; and

(C) by striking subparagraph (F);

(4) by striking subsection (d);

by redesignating subsections through (i) as subsections (d) through (h), re-

(6) by amending subsection (e), as redesignated by paragraph (5) of this section, to read as follows:

"(e)(1) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General-

"(A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained:

"(B) reasonably determines that the factual basis for the issuance of an order under this title to approve such electronic surveillance exists:

"(C) informs, either personally or through a designee, a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

"(D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance.

"(2) If the Attorney General authorizes the emergency employment of electronic surveillance under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for issuance of a judicial order be followed.

"(3) In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest

"(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

"(5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

"(6) The Attorney General shall assess compliance with the requirements of paragraph (5)."; and

(7) by adding at the end the following:

"(i) In any case in which the Government makes an application to a judge under this title to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 402(d)(2).".

(b) CONFORMING AMENDMENT.—Section 108(a)(2)(C) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1808(a)(2)(C)) is amended by striking "105(f)" and inserting "105(e)":

SEC. 106. USE OF INFORMATION.

June 20, 2008

Subsection (i) of section 106 of the Foreign Intelligence Surveillance Act of 1978 (8 U.S.C. 1806) is amended by striking "radio communication" and inserting "communication".

SEC. 107. AMENDMENTS FOR PHYSICAL SEARCHES.

- (a) APPLICATIONS.—Section 303 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1823) is amended—
 - (1) in subsection (a)—
 - (A) by striking paragraph (2);
- (B) by redesignating paragraphs (3) through (9) as paragraphs (2) through (8), respectively:
- (C) in paragraph (2), as redesignated by subparagraph (B) of this paragraph, by striking "detailed":
- (D) in paragraph (3)(C), as redesignated by subparagraph (B) of this paragraph, by inserting "or is about to be" before "owned"; and
- (E) in paragraph (6), as redesignated by subparagraph (B) of this paragraph, in the matter preceding subparagraph (A)—
- (i) by striking "Affairs or" and inserting "Affairs,"; and
- (ii) by striking "Senate—" and inserting "Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—"; and
- (2) in subsection (d)(1)(A), by striking "or the Director of National Intelligence" and inserting "the Director of National Intelligence, or the Director of the Central Intelligence Agency".
- (b) ORDERS.—Section 304 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824) is amended—
 - (1) in subsection (a)—
 - (A) by striking paragraph (1);
- (B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively; and
- (C) in paragraph (2)(B), as redesignated by subparagraph (B) of this paragraph, by inserting "or is about to be" before "owned"; and
- (2) by amending subsection (e) to read as follows:
- "(e)(1) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of a physical search if the Attorney General—
- "(A) reasonably determines that an emergency situation exists with respect to the employment of a physical search to obtain foreign intelligence information before an order authorizing such physical search can with due diligence be obtained:
- "(B) reasonably determines that the factual basis for issuance of an order under this title to approve such physical search exists;
- "(C) informs, either personally or through a designee, a judge of the Foreign Intelligence Surveillance Court at the time of such authorization that the decision has been made to employ an emergency physical search; and
- "(D) makes an application in accordance with this title to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such physical search.
- "(2) If the Attorney General authorizes the emergency employment of a physical search under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.

"(3) In the absence of a judicial order approving such physical search, the physical search shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

"(4) A denial of the application made under this subsection may be reviewed as provided

in section 103.

- (5) In the event that such application for approval is denied, or in any other case where the physical search is terminated and no order is issued approving the physical search, no information obtained or evidence derived from such physical search shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such physical search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.
- "(6) The Attorney General shall assess compliance with the requirements of paragraph (5).".
- (c) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—
- (1) in section 304(a)(4), as redesignated by subsection (b) of this section, by striking "303(a)(7)(E)" and inserting "303(a)(6)(E)"; and
- (2) in section 305(k)(2), by striking "303(a)(7)" and inserting "303(a)(6)".

SEC. 108. AMENDMENTS FOR EMERGENCY PEN REGISTERS AND TRAP AND TRACE DEVICES.

Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended—

- (1) in subsection (a)(2), by striking "48 hours" and inserting "7 days"; and
- (2) in subsection (c)(1)(C), by striking "48 hours" and inserting "7 days".

SEC. 109. FOREIGN INTELLIGENCE SURVEIL-LANCE COURT.

- (a) DESIGNATION OF JUDGES.—Subsection (a) of section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended by inserting "at least" before "seven of the United States judicial circuits".
 - (b) EN BANC AUTHORITY.—
- (1) IN GENERAL.—Subsection (a) of section 103 of the Foreign Intelligence Surveillance Act of 1978, as amended by subsection (a) of this section, is further amended—
- (A) by inserting "(1)" after "(a)"; and
- (B) by adding at the end the following new paragraph:
- "(2)(A) The court established under this subsection may, on its own initiative, or upon the request of the Government in any proceeding or a party under section 501(f) or paragraph (4) or (5) of section 702(h), hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that—
- "(i) en banc consideration is necessary to secure or maintain uniformity of the court's decisions; or
- "(ii) the proceeding involves a question of exceptional importance
- "(B) Any authority granted by this Act to a judge of the court established under this subsection may be exercised by the court en banc. When exercising such authority, the court en banc shall comply with any requirements of this Act on the exercise of such authority.

- "(C) For purposes of this paragraph, the court en banc shall consist of all judges who constitute the court established under this subsection."
- (2) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 is further amended—
- (A) in subsection (a) of section 103, as amended by this subsection, by inserting "(except when sitting en banc under paragraph (2))" after "no judge designated under this subsection"; and
- (B) in section 302(c) (50 U.S.C. 1822(c)), by inserting "(except when sitting en banc)" after "except that no judge".
- (c) STAY OR MODIFICATION DURING AN APPEAL.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended—
- (1) by redesignating subsection (f) as subsection (g); and
- (2) by inserting after subsection (e) the following new subsection:
- "(f)(1) A judge of the court established under subsection (a), the court established under subsection (b) or a judge of that court, or the Supreme Court of the United States or a justice of that court, may, in accordance with the rules of their respective courts, enter a stay of an order or an order modifying an order of the court established under subsection (a) or the court established under subsection (b) entered under any title of this Act, while the court established under subsection (a) conducts a rehearing, while an appeal is pending to the court established under subsection (b), or while a petition of certiorari is pending in the Supreme Court of the United States, or during the pendency of any review by that court.
- "(2) The authority described in paragraph (1) shall apply to an order entered under any provision of this Act.".
- (d) AUTHORITY OF FOREIGN INTELLIGENCE SURVEILLANCE COURT.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803), as amended by this Act, is amended by adding at the end the following:
- "(i) Nothing in this Act shall be construed to reduce or contravene the inherent authority of the court established under subsection (a) to determine or enforce compliance with an order or a rule of such court or with a procedure approved by such court."

SEC. 110. WEAPONS OF MASS DESTRUCTION.

- (a) Definitions.—
- (1) FOREIGN POWER.—Subsection (a) of section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(a)) is amended—
- (A) in paragraph (5), by striking "persons; or" and inserting "persons;";
- (B) in paragraph (6) by striking the period and inserting "; or"; and
- (C) by adding at the end the following new paragraph:
- "(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction."
- (2) AGENT OF A FOREIGN POWER.—Subsection (b)(1) of such section 101 is amended—
- (A) in subparagraph (B), by striking "or" at the end;
- (B) in subparagraph (C), by striking "or" at the end; and
- (C) by adding at the end the following new subparagraphs:
- "(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or
- "(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or".
- (3) FOREIGN INTELLIGENCE INFORMATION.—Subsection (e)(1)(B) of such section 101 is

- amended by striking "sabotage or international terrorism" and inserting "sabotage, international terrorism, or the international proliferation of weapons of mass destruction".
- (4) WEAPON OF MASS DESTRUCTION.—Such section 101 is amended by adding at the end the following new subsection:
- "(1) any explosive, incendiary, or poison
- "(1) any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a mass casualty incident:
- "(2) any weapon that is designed, intended, or has the capability to cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors:
- "(3) any weapon involving a biological agent, toxin, or vector (as such terms are defined in section 178 of title 18, United States Code) that is designed, intended, or has the capability to cause death, illness, or serious bodily injury to a significant number of persons; or
- "(4) any weapon that is designed, intended, or has the capability to release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons."
 - (b) Use of Information .-
- (1) In GENERAL.—Section 106(k)(1)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806(k)(1)(B)) is amended by striking "sabotage or international terrorism" and inserting "sabotage, international terrorism, or the international proliferation of weapons of mass destruction".
- (2) PHYSICAL SEARCHES.—Section 305(k)(1)(B) of such Act (50 U.S.C. 1825(k)(1)(B)) is amended by striking "sabotage or international terrorism" and inserting "sabotage, international terrorism, or the international proliferation of weapons of mass destruction".
- (c) TECHNICAL AND CONFORMING AMEND-MENTS.—The Foreign Intelligence Surveillance Act of 1978 is further amended—
- (1) in paragraph (2) of section 105(d) (50 U.S.C. 1805(d)), as redesignated by section 105(a)(5) of this Act, by striking "section 101(a) (5) or (6)" and inserting "paragraph (5), (6), or (7) of section 101(a)";
- (2) in section 301(1) (50 U.S.C. 1821(1)), by inserting "weapon of mass destruction," after "person,"; and
- (3) in section 304(d)(2) (50 U.S.C. 1824(d)(2)), by striking "section 101(a) (5) or (6)" and inserting "paragraph (5), (6), or (7) of section 101(a)".

TITLE II—PROTECTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS

SEC. 201. PROCEDURES FOR IMPLEMENTING STATUTORY DEFENSES UNDER THE FOREIGN INTELLIGENCE SURVEIL-LANCE ACT OF 1978.

The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by section 101, is further amended by adding at the end the following new title:

"TITLE VIII—PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

"SEC. 801. DEFINITIONS.

"In this title:

- "(1) Assistance.—The term 'assistance' means the provision of, or the provision of access to, information (including communication contents, communications records, or other information relating to a customer or communication), facilities, or another form of assistance.
- "(2) CIVIL ACTION.—The term 'civil action' includes a covered civil action.
- "(3) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term 'congressional intelligence committees' means—

- "(A) the Select Committee on Intelligence of the Senate; and
- "(B) the Permanent Select Committee on Intelligence of the House of Representatives.
 "(4) CONTENTS.—The term 'contents' has
- "(4) CONTENTS.—The term 'contents' has the meaning given that term in section 101(n).
- ''(5) COVERED CIVIL ACTION.—The term 'covered civil action' means a civil action filed in a Federal or State court that—
- "(A) alleges that an electronic communication service provider furnished assistance to an element of the intelligence community; and
- "(B) seeks monetary or other relief from the electronic communication service provider related to the provision of such assistance.
- "(6) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term 'electronic communication service provider' means—
- "(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);
- "(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;
- "(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18. United States Code:
- "(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored;
- "(E) a parent, subsidiary, affiliate, successor, or assignee of an entity described in subparagraph (A), (B), (C), or (D); or
- "(F) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), (D), or (E).
- "(7) INTELLIGENCE COMMUNITY.—The term intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).
- "(8) PERSON.—The term 'person' means—
- "(A) an electronic communication service provider; or
- "(B) a landlord, custodian, or other person who may be authorized or required to furnish assistance pursuant to—
- "(i) an order of the court established under section 103(a) directing such assistance;
- "(ii) a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code: or
- "(iii) a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), or 702(h)
- "(9) STATE.—The term 'State' means any State, political subdivision of a State, the Commonwealth of Puerto Rico, the District of Columbia, and any territory or possession of the United States, and includes any officer, public utility commission, or other body authorized to regulate an electronic communication service provider.

"SEC. 802. PROCEDURES FOR IMPLEMENTING STATUTORY DEFENSES.

- "(a) REQUIREMENT FOR CERTIFICATION.— Notwithstanding any other provision of law, a civil action may not lie or be maintained in a Federal or State court against any person for providing assistance to an element of the intelligence community, and shall be promptly dismissed, if the Attorney General certifies to the district court of the United States in which such action is pending that—
- "(1) any assistance by that person was provided pursuant to an order of the court established under section 103(a) directing such assistance:
- "(2) any assistance by that person was provided pursuant to a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code;

- "(3) any assistance by that person was provided pursuant to a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007 (Public Law 110–55), or 702(h) directing such assistance;
- "(4) in the case of a covered civil action, the assistance alleged to have been provided by the electronic communication service provider was—
- "(A) in connection with an intelligence activity involving communications that was—
- "(i) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and
- "(ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and
- "(B) the subject of a written request or directive, or a series of written requests or directives, from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was—
 - "(i) authorized by the President; and
 - "(ii) determined to be lawful: or
- "(5) the person did not provide the alleged assistance.
 - "(b) JUDICIAL REVIEW.—
- "(1) REVIEW OF CERTIFICATIONS.—A certification under subsection (a) shall be given effect unless the court finds that such certification is not supported by substantial evidence provided to the court pursuant to this section.
- "(2) SUPPLEMENTAL MATERIALS.—In its review of a certification under subsection (a), the court may examine the court order, certification, written request, or directive described in subsection (a) and any relevant court order, certification, written request, or directive submitted pursuant to subsection (d)
- Attorney General files a declaration under section 1746 of title 28, United States Code, that disclosure of a certification made pursuant to subsection (a) or the supplemental materials provided pursuant to subsection (b) or (d) would harm the national security of the United States, the court shall—
- "(1) review such certification and the supplemental materials in camera and ex parte; and
- "(2) limit any public disclosure concerning such certification and the supplemental materials, including any public order following such in camera and ex parte review, to a statement as to whether the case is dismissed and a description of the legal standards that govern the order, without disclosing the paragraph of subsection (a) that is the basis for the certification.
- (d) Role of the Parties.—Any plaintiff or defendant in a civil action may submit any relevant court order, certification, written request, or directive to the district court referred to in subsection (a) for review and shall be permitted to participate in the briefing or argument of any legal issue in a judicial proceeding conducted pursuant to this section, but only to the extent that such participation does not require the disclosure of classified information to such party. To the extent that classified information is relevant to the proceeding or would be revealed in the determination of an issue, the court shall review such information in camera and ex parte, and shall issue any part of the court's written order that would reveal classified information in camera and ex parte and maintain such part under seal.
- "(e) NONDELEGATION.—The authority and duties of the Attorney General under this section shall be performed by the Attorney General (or Acting Attorney General) or the Deputy Attorney General.

- "(f) APPEAL.—The courts of appeals shall have jurisdiction of appeals from interlocutory orders of the district courts of the United States granting or denying a motion to dismiss or for summary judgment under this section.
- "(g) REMOVAL.—A civil action against a person for providing assistance to an element of the intelligence community that is brought in a State court shall be deemed to arise under the Constitution and laws of the United States and shall be removable under section 1441 of title 28, United States Code.

"(h) RELATIONSHIP TO OTHER LAWS.—Nothing in this section shall be construed to limit any otherwise available immunity, privilege, or defense under any other provision of law.

"(i) APPLICABILITY.—This section shall apply to a civil action pending on or filed after the date of the enactment of the FISA Amendments Act of 2008.

"SEC. 803. PREEMPTION.

- "(a) IN GENERAL.—No State shall have authority to—
- "(1) conduct an investigation into an electronic communication service provider's alleged assistance to an element of the intelligence community;
- "(2) require through regulation or any other means the disclosure of information about an electronic communication service provider's alleged assistance to an element of the intelligence community;
- "(3) impose any administrative sanction on an electronic communication service provider for assistance to an element of the intelligence community; or
- "(4) commence or maintain a civil action or other proceeding to enforce a requirement that an electronic communication service provider disclose information concerning alleged assistance to an element of the intelligence community.

"(b) SUITS BY THE UNITED STATES.—The United States may bring suit to enforce the provisions of this section.

"(c) JURISDICTION.—The district courts of the United States shall have jurisdiction over any civil action brought by the United States to enforce the provisions of this sec-

"(d) APPLICATION.—This section shall apply to any investigation, action, or proceeding that is pending on or commenced after the date of the enactment of the FISA Amendments Act of 2008.

"SEC. 804. REPORTING.

- "(a) SEMIANNUAL REPORT.—Not less frequently than once every 6 months, the Attorney General shall, in a manner consistent with national security, the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution, fully inform the congressional intelligence committees, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives concerning the implementation of this title.
- "(b) CONTENT.—Each report made under subsection (a) shall include—
- "(1) any certifications made under section 802;
- "(2) a description of the judicial review of the certifications made under section 802;
- "(3) any actions taken to enforce the provisions of section 803.".

SEC. 202. TECHNICAL AMENDMENTS.

The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by section 101(b), is further amended by adding at the end the following:

"TITLE VIII—PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

"Sec. 801. Definitions.

- "Sec. 802. Procedures for implementing statutory defenses.
- "Sec. 803. Preemption.
- "Sec. 804. Reporting."

TITLE III—REVIEW OF PREVIOUS ACTIONS SEC. 301. REVIEW OF PREVIOUS ACTIONS.

- (a) DEFINITIONS.—In this section:
- (1) APPROPRIATE COMMITTEES OF CONGRESS.—The term "appropriate committees of Congress" means—
- (A) the Select Committee on Intelligence and the Committee on the Judiciary of the Senate; and
- (B) the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives.
- (2) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term "Foreign Intelligence Surveillance Court" means the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)).
- (3) PRESIDENT'S SURVEILLANCE PROGRAM AND PROGRAM.—The terms "President's Surveillance Program" and "Program" mean the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005 (commonly known as the Terrorist Surveillance Program).
- (b) Reviews.—
- (1) REQUIREMENT TO CONDUCT.—The Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other element of the intelligence community that participated in the President's Surveillance Program, shall complete a comprehensive review of, with respect to the oversight authority and responsibility of each such Inspector General—
- (A) all of the facts necessary to describe the establishment, implementation, product, and use of the product of the Program;
- (B) access to legal reviews of the Program and access to information about the Program:
- (C) communications with, and participation of, individuals and entities in the private sector related to the Program;
- (D) interaction with the Foreign Intelligence Surveillance Court and transition to court orders related to the Program; and
- (E) any other matters identified by any such Inspector General that would enable that Inspector General to complete a review of the Program, with respect to such Department or element.
- (2) COOPERATION AND COORDINATION.—
- (A) COOPERATION.—Each Inspector General required to conduct a review under paragraph (1) shall—
- (i) work in conjunction, to the extent practicable, with any other Inspector General required to conduct such a review; and
- (ii) utilize, to the extent practicable, and not unnecessarily duplicate or delay, such reviews or audits that have been completed or are being undertaken by any such Inspector General or by any other office of the Executive Branch related to the Program.
- (B) INTEGRATION OF OTHER REVIEWS.—The Counsel of the Office of Professional Responsibility of the Department of Justice shall provide the report of any investigation conducted by such Office on matters relating to the Program, including any investigation of the process through which legal reviews of the Program were conducted and the substance of such reviews, to the Inspector General of the Department of Justice, who shall integrate the factual findings and conclusions of such investigation into its review.

- (C) COORDINATION.—The Inspectors General shall designate one of the Inspectors General required to conduct a review under paragraph (1) that is appointed by the President, by and with the advice and consent of the Senate, to coordinate the conduct of the reviews and the preparation of the reports.
 - (c) Reports.-
- (1) PRELIMINARY REPORTS.—Not later than 60 days after the date of the enactment of this Act, the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other Inspector General required to conduct a review under subsection (b)(1), shall submit to the appropriate committees of Congress an interim report that describes the planned scope of such review.
- (2) FINAL REPORT.—Not later than 1 year after the date of the enactment of this Act, the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other Inspector General required to conduct a review under subsection (b)(1), shall submit to the appropriate committees of Congress, in a manner consistent with national security, a comprehensive report on such reviews that includes any recommendations of any such Inspector General within the oversight authority and responsibility of any such Inspector General with respect to the reviews.
- (3) FORM.—A report under this subsection shall be submitted in unclassified form, but may include a classified annex. The unclassified report shall not disclose the name or identity of any individual or entity of the private sector that participated in the Program or with whom there was communication about the Program, to the extent that information is classified.
 - (d) Resources .-
- (1) EXPEDITED SECURITY CLEARANCE.—The Director of National Intelligence shall ensure that the process for the investigation and adjudication of an application by an Inspector General or any appropriate staff of an Inspector General for a security clearance necessary for the conduct of the review under subsection (b)(1) is carried out as expeditiously as possible.
- (2) Additional personnel for the inspectors general.—An inspector General required to conduct a review under subsection (b)(1) and submit a report under subsection (c) is authorized to hire such additional personnel as may be necessary to carry out such review and prepare such report in a prompt and timely manner. Personnel authorized to be hired under this paragraph—
- (A) shall perform such duties relating to such a review as the relevant Inspector General shall direct; and
- (B) are in addition to any other personnel authorized by law.
- (3) TRANSFER OF PERSONNEL.—The Attorney General, the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, or the head of any other element of the intelligence community may transfer personnel to the relevant Office of the Inspector General required to conduct a review under subsection (b)(1) and submit a report under subsection (c) and, in addition to any other personnel authorized by law, are authorized to fill any vacancy caused by such a transfer. Personnel transferred under this paragraph shall perform such duties relating to such review as the relevant Inspector General shall direct.

TITLE IV—OTHER PROVISIONS

SEC. 401. SEVERABILITY.

If any provision of this Act, any amendment made by this Act, or the application thereof to any person or circumstances is

held invalid, the validity of the remainder of the Act, of any such amendments, and of the application of such provisions to other persons and circumstances shall not be affected thereby.

SEC. 402. EFFECTIVE DATE.

Except as provided in section 404, the amendments made by this Act shall take effect on the date of the enactment of this Act. SEC. 403. REPEALS.

- (a) Repeal of Protect America Act of 2007 Provisions.—
 - (1) AMENDMENTS TO FISA.—
- (A) IN GENERAL.—Except as provided in section 404, sections 105A, 105B, and 105C of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805a, 1805b, and 1805c) are repealed.
- (B) TECHNICAL AND CONFORMING AMEND-MENTS —
- (i) TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by striking the items relating to sections 105A, 105B, and 105C.
- (ii) CONFORMING AMENDMENTS.—Except as provided in section 404, section 103(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(e)) is amended—
- (I) in paragraph (1), by striking "105B(h) or 501(f)(1)" and inserting "501(f)(1) or 702(h)(4)"; and
- (II) in paragraph (2), by striking "105B(h) or 501(f)(1)" and inserting "501(f)(1) or 702(h)(4)".
- (2) REPORTING REQUIREMENTS.—Except as provided in section 404, section 4 of the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 555) is repealed.
- (3) Transition Procedures.—Except as provided in section 404, subsection (b) of section 6 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 556) is repealed.
- (b) FISA AMENDMENTS ACT OF 2008.—
 (1) IN GENERAL.—Except as provided in section 404, effective December 31, 2012, title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), is re-
- pealed.
 (2) Technical and conforming amendments.—Effective December 31, 2012—
- (A) the table of contents in the first section of such Act (50 U.S.C. 1801 et seq.) is amended by striking the items related to title VII;
- (B) except as provided in section 404, section 601(a)(1) of such Act (50 U.S.C. 1871(a)(1)) is amended to read as such section read on the day before the date of the enactment of this Act; and
- (C) except as provided in section 404, section 2511(2)(a)(ii)(A) of title 18, United States Code, is amended by striking "or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978".

SEC. 404. TRANSITION PROCEDURES.

- (a) Transition Procedures for Protect America Act of 2007 Provisions.—
- (1) CONTINUED EFFECT OF ORDERS, AUTHORIZATIONS, DIRECTIVES.—Except as provided in paragraph (7), notwithstanding any other provision of law, any order, authorization, or directive issued or made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 552), shall continue in effect until the expiration of such order, authorization, or directive.
- (2) APPLICABILITY OF PROTECT AMERICA ACT OF 2007 TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—
- (A) subject to paragraph (3), section 105A of such Act, as added by section 2 of the Pro-

tect America Act of 2007 (Public Law 110-55; 121 Stat. 552), shall continue to apply to any acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1); and

- (B) sections 105B and 105C of the Foreign Intelligence Surveillance Act of 1978, as added by sections 2 and 3, respectively, of the Protect America Act of 2007, shall continue to apply with respect to an order, authorization, or directive referred to in paragraph (1) until the later of—
- (i) the expiration of such order, authorization, or directive; or
- (ii) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive
- (3) USE OF INFORMATION.—Information acquired from an acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1) shall be deemed to be information acquired from an electronic surveillance pursuant to title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) for purposes of section 106 of such Act (50 U.S.C. 1806), except for purposes of subsection (j) of such section.
- (4) PROTECTION FROM LIABILITY.—Subsection (1) of section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, shall continue to apply with respect to any directives issued pursuant to such section 105B.
- (5) JURISDICTION OF FOREIGN INTELLIGENCE SURVEILLANCE COURT.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 103(e) of the Foreign Intelligence Surveillance Act (50 U.S.C. 1803(e)), as amended by section 5(a) of the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 556), shall continue to apply with respect to a directive issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, until the later of—
- (A) the expiration of all orders, authorizations, or directives referred to in paragraph (1); or
- (B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.
 - (6) REPORTING REQUIREMENTS.—
- (A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act, any amendment made by this Act, the Protect America Act of 2007 (Public Law 110-55), or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 4 of the Protect America Act of 2007 shall continue to apply until the date that the certification described in subparagraph (B) is submitted.
- (B) CERTIFICATION.—The certification described in this subparagraph is a certification—
- (i) made by the Attorney General;
- (ii) submitted as part of a semi-annual report required by section 4 of the Protect America Act of 2007;
- (iii) that states that there will be no further acquisitions carried out under section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, after the date of such certification; and
- (iv) that states that the information required to be included under such section 4 relating to any acquisition conducted under such section 105B has been included in a semi-annual report required by such section
- (7) REPLACEMENT OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—

- (A) IN GENERAL.—If the Attorney General and the Director of National Intelligence seek to replace an authorization issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), with an authorization under section 702 of the Foreign Intelligence Surveillance Act of 1978 (as added by section 101(a) of this Act), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of such Act (as so added)) a certification prepared in accordance with subsection (g) of such section 702 and the procedures adopted in accordance with subsections (d) and (e) of such section 702 at least 30 days before the expiration of such authorization.
- (B) CONTINUATION OF EXISTING ORDERS.—If the Attorney General and the Director of National Intelligence seek to replace an authorization made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 522), by filing a certification in accordance with subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a) of such section 105B, until the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of the Foreign Intelligence Surveillance Act of 1978 (as so added)) issues an order with respect to that certification under section 702(i)(3) of such Act (as so added) at which time the provisions of that section and of section 702(i)(4) of such Act (as so added) shall apply.
- (8) EFFECTIVE DATE.—Paragraphs (1) through (7) shall take effect as if enacted on August 5, 2007.
- (b) Transition Procedures for FISA Amendments Act of 2008 Provisions.—
- (1) ORDERS IN EFFECT ON DECEMBER 31, 2012.—
 Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), any order, authorization, or directive issued or made under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), shall continue in effect until the date of the expiration of such order, authorization, or directive.
- (2) APPLICABILITY OF TITLE VII OF FISA TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), with respect to any order, authorization, or directive referred to in paragraph (1), title VII of such Act, as amended by section 101(a), shall continue to apply until the later of—
- (A) the expiration of such order, authorization, or directive; or
- (B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive
- (3) CHALLENGE OF DIRECTIVES; PROTECTION FROM LIABILITY; USE OF INFORMATION.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—
- (A) section 103(e) of such Act, as amended by section 403(a)(1)(B)(ii), shall continue to apply with respect to any directive issued pursuant to section 702(h) of such Act, as added by section 101(a);
- (B) section 702(h)(3) of such Act (as so added) shall continue to apply with respect to any directive issued pursuant to section 702(h) of such Act (as so added);

- (C) section 703(e) of such Act (as so added) shall continue to apply with respect to an order or request for emergency assistance under that section;
- (D) section 706 of such Act (as so added) shall continue to apply to an acquisition conducted under section 702 or 703 of such Act (as so added); and
- (E) section 2511(2)(a)(ii)(A) of title 18, United States Code, as amended by section 101(c)(1), shall continue to apply to an order issued pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978, as added by section 101(a).
 - (4) REPORTING REQUIREMENTS.—
- (A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 601(a) of such Act (50 U.S.C. 1871(a)), as amended by section 101(c)(2), and sections 702(1) and 707 of such Act, as added by section 101(a), shall continue to apply until the date that the certification described in subparagraph (B) is submitted.
- (B) CERTIFICATION.—The certification described in this subparagraph is a certification—
- (i) made by the Attorney General:
- (ii) submitted to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committees on the Judiciary of the Senate and the House of Representatives;
- (iii) that states that there will be no further acquisitions carried out under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), after the date of such certification; and
- (iv) that states that the information required to be included in a review, assessment, or report under section 601 of such Act, as amended by section 101(c), or section 702(1) or 707 of such Act, as added by section 101(a), relating to any acquisition conducted under title VII of such Act, as amended by section 101(a), has been included in a review, assessment, or report under such section 601, 702(1), or 707.
- (5) Transition procedures concerning the targeting of united states persons overseas.—Any authorization in effect on the date of enactment of this Act under section 2.5 of Executive Order 12333 to intentionally target a United States person reasonably believed to be located outside the United States shall continue in effect, and shall constitute a sufficient basis for conducting such an acquisition targeting a United States person located outside the United States until the earlier of—
- (A) the date that authorization expires; or (B) the date that is 90 days after the date of the enactment of this Act.

The SPEAKER pro tempore. Pursuant to House Resolution 1285, debate shall not exceed 1 hour, with 30 minutes equally divided and controlled by the chairman and ranking minority member of the Committee on the Judiciary, and 30 minutes equally divided and controlled by the chairman and ranking minority member of the Permanent Select Committee on Intelligence.

The gentleman from Michigan (Mr. CONYERS), the gentleman from Texas (Mr. SMITH), the gentleman from Texas (Mr. REYES), and the gentleman from Michigan (Mr. HOEKSTRA) each will control 15 minutes.

The Chair recognizes the gentleman from Michigan (Mr. CONYERS).

GENERAL LEAVE

Mr. CONYERS. Madam Speaker, I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and include extraneous material on the bill under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Michigan?

There was no objection.

Mr. CONYERS. Madam Speaker, I yield myself such time as I may consume

Members of the House, several months ago on October 16, 2007, to be exact, the House passed the Foreign Intelligence Surveillance Act legislation, known as the RESTORE Act. In the view of this Member, the RESTORE Act was a reasonable and balanced one giving the administration the power it needs to combat terrorism while protecting our precious rights and liberties.

The legislation before us today, which I concede includes significant improvements over the Senate legislation, goes beyond what I think was a reasonable bottom line in the form of the RESTORE Act.

Title I of the bill continues the House approach by providing mechanisms to ensure that FISA's longstanding exclusivity is crystal clear. It states only a new statute directly addressing the executive branch's foreign intelligence surveillance authority can modify FISA. Secondly, it provides sunshine by requiring that the government requests to private parties for surveillance assistance must actually cite the statutory authority under which they're issued.

Now in earlier versions of FISA reform, the administration claimed that prior court approval of procedures for overseas surveillance would hurt national security. This matter is now laid to rest with the consensus that upfront court review is indeed appropriate. The requirement for individual warrants and probable cause determinations for Americans overseas is an improvement over even the original FISA legislation. There is a provision in the legislation that permits the Attorney General and Director of National Intelligence to begin surveillance prior to seeking court approval for the necessary procedures in exigent circumstances. This is intended to be used rarely, if at all, and was included upon assurances from the administration that agrees that it shall not be used routinely.

The measure before us further requires extensive oversight by Congress and the independent Inspectors General to prevent abuse. It mandates guidelines for targeting minimization and to prevent reverse targeting and tasks the Inspector General to monitor compliance with those protections.

Now title II of the legislation concerning telecom liability raises the most serious concerns in my view. In the past, I have said I would be open to developing a set of procedures that

allow both plaintiffs and defendants to make their case. Unfortunately, this bill goes well beyond that and changes the substantive standard for legal liability by the telecom community, by the telecom companies and does so on a retroactive basis, retroactive immunity. And so I appreciate that the final bill does not send the matter to a new secret court and does grant the court a meaningful role in the determination. Unfortunately, these improvements do not redeem the overall provision.

Title III of the bill will also ask the Inspector General to conduct independent investigations into the President's warrantless wiretapping program. This inquiry will help uncover the truth for the American people, hopefully, about the President's activities. And then there is a part in here about an emergency provision any U.S. citizen can be wiretapped. And I strenuously object to that.

Six years ago, the Administration unilaterally chose to engage in warrantless surveillance of American citizens without court review. We are now restoring the balance through enhanced Congressional oversight, Inspector General investigations, and procedures to ensure that FISA remains the exclusive means for authorizing electronic surveillance.

This bill continues the House approach by providing mechanisms to ensure that FISA's longstanding exclusivity is crystal clear. First, it states that only a new statute directly addressing the executive branch's foreign intelligence surveillance authority can modify FISA. Secondly, it provides sunshine by requiring requests for assistance to cite the statutory authority under which they are issued. A conforming amendment to Title 18 Section 2511(2)(a) is meant to underscore the need to specify the specific statutory language being relied on, and must be read in conjunction with the entirety of Sec. 102 of the legislation. It should not be read to imply that assistance may be sought for electronic surveillance, as defined in the statute, which is not specifically authorized by statute.

In earlier versions of FISA reform, the Administration claimed that prior court approval of procedures for overseas surveillance would hurt national security. This matter is now laid to rest, with a consensus that up-front court review is in fact appropriate. The requirement for individual warrants and probable cause determinations for Americans overseas is an improvement over even the original FISA legislation.

There is a provision in the legislation that permits the Attorney General and Director of National Intelligence to begin a surveillance prior to seeking court approval for the necessary procedures in "exigent circumstances." This is intended to be used rarely, if at all. In the normal course of events the DNI will have ample time to submit such procedures to the FISA court for its approval before initiating a particular surveillance.

The Congress provided this authority at the request of the DNI to meet unforeseen and extraordinary circumstances, and the Administration agrees that it may not be used routinely. The Administration understands that the Congress expects its use to be very rare if it is used at all.

The oversight committees will be informed of any use of the exigent circumstances provision and are committed to effective oversight to insure that it is not used to avoid the requirement to secure court approval of the procedures in advance in all but the most extreme circumstances. The exception must not swallow the rule.

The bill requires extensive oversight by Congress and the independent Inspectors General to prevent abuse. It mandates guidelines for targeting, minimization, and to prevent reverse targeting, and tasks the Inspectors General to monitor compliance with those protections.

"Reverse targeting" is specifically prohibited in Section 702(b)(2). The Intelligence Community agrees that this language prohibits the targeting of one or more persons overseas for the purpose of acquiring the communications of a specific is person reasonably believed to be in the United States. Thus, Section 702(f) requires the government to adopt guidelines to insure that this abuse does not occur and the FISA court must review and approve these guidelines and assure that they are consistent with the Fourth Amendment. The oversight committees of the Congress intend to conduct rigorous oversight to insure that these provisions are faithfully observed. In this connection the Committee attaches particular importance to the required annual review and the reporting in that review of the number of disseminated reports which contain a reference to the identity of a US person.

There is currently ongoing multi-District litigation in which a federal District Court is conducting a review of the telecom carriers' activities and the lawfulness of the President's warrantless wiretapping program. This bill does not strip jurisdiction on that Court and provide blanket immunity, as many wanted.

Instead, in cases where the program was actually designed to detect or prevent a terrorist attack, the Court will assess an Attorney General certification that can assert—among other reasons for dismissal-that the carriers got certain requests and directives from the Administration. The Court will look to see if the Attorney General's certification is backed up with substantial evidence. That means not only the underlying directives and requests, but supplemental materials as well. And in cases where the Government claims that the company did not provide the alleged assistance, a bald assertion is not "substantial evidence"—the Government will have to back up its claims to the Court's satisfaction.

That Title II of this bill provides procedures for assessing lawsuits relating to warrantless surveillance since 9/11 does not imply that such surveillance was lawful or that the Congress as a whole believes that the service providers acted lawfully in providing assistance. Nor can the provision remove the power of the courts hearing the cases to determine if this provision is constitutional.

No company or private citizen asked by the executive branch to provide assistance in securing the private information of Americans without authority of law should read this language as implying that Congress will act in the future to provide such a grounds for dismissing a lawsuit. On the contrary, companies should be on notice that the Congress is very reluctantly providing this defense as a one-time action in an extremely unusual circumstance. It expects private citizens and

companies to provide assistance only when specifically authorized by law.

For over 30 years we have mandated that telecommunications carriers not be a merely unquestioning partner to surveillance activities. This bill provides many ways for the companies to question or challenge directives or requests for assistance, and we expect these to be used any time there is something unusual or novel being requested.

Today's compromise will give the District Court direction and procedures for handling the pending lawsuits. However, it is important to note that the question of whether FISA's existing security procedures at 50 U.S.C. 1806(f) preempt the state secrets privilege is still being litigated in the courts in a case against the Government. Nothing in this bill is intended to affect that litigation, or any litigation against the Government or Government employees.

Today's vote is not the end of the matter. The bill provides for a 4-year sunset, but this doesn't mean we cannot or should not revisit these issues in the next congressional session. We will conduct vigorous oversight, and will be monitoring the program through the reports and audits. We will be keeping a close eye on the development and implementation of reverse targeting, minimization, and targeting procedures, in order to not only make sure that they are followed, but to inform us as we consider what improvements need to be made to this legislation.

On that note, I will reserve the balance of my time.

Mr. SMITH of Texas. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, after nearly a year of delays and months of negotiations, the House today will finally vote on compromise legislation that gives our intelligence community the tools that it needs to protect America. I join my colleague, Mr. HOEKSTRA, ranking member of the Intelligence Committee, and Chairman REYES, as an original cosponsor of this compromise bill.

America's enemies take on many forms, terrorist groups, foreign governments and spies who all pose serious threat to America and its allies. Last August, Congress passed the Protect America Act which provided a temporary solution to the problem. The PAA expired in February. As a result, our intelligence community could not gather two-thirds of the foreign intelligence they needed to protect American lives.

From day one, we insisted that any legislation passed by Congress must not interfere with our fundamental ability to collect foreign intelligence. This legislation accomplishes that goal. H.R. 6304 does not extend constitutional protections to foreign terrorists and other foreign targets overseas. The bill does allow the intelligence community to target a foreign person overseas without a court order if critical intelligence would be lost or not collected in a timely manner.

We insisted that any legislation passed by Congress include strong liability protections for telecommunications carriers that assisted the government following the terrorist attacks of September 11, 2001, as well as protections for their assistance in the future. H.R. 6304 provides these important protections.

We insisted that Congress enact longterm FISA legislation. The bill we have before us today will not sunset until the end of 2012. This compromise legislation also provides strong civil liberties protections for Americans both within the United States and abroad. And it mandates congressional oversight and detailed reports to the House and Senate Judiciary and Intelligence committees and requires a review by the Inspectors General of the Department of Justice and the intelligence agencies. This compromise is long overdue. It is supported by both the Department of Justice and the intelligence community.

Madam Speaker, I urge my colleagues to support this bill.

Madam Speaker, I submit the following letter for the RECORD:

JUNE 19, 2008.

Hon. NANCY PELOSI, Speaker, House of Representatives, Washington, DC.

DEAR-MADAM SPEAKER: This letter presents the views of the Administration on the Foreign Intelligence Surveillance Act of 1978 ("FISA") Amendments Act of 2008 (H.R. 6304). The bill would modernize FISA to reflect changes in communications technology since the Act was first passed 30 years ago. The amendments would provide the Intelligence Community with the tools it needs to collect the foreign intelligence necessary to secure our Nation while protecting the civil liberties of Americans. The bill would also provide the necessary legal protections for those companies sued because they are believed to have helped the Government prevent terrorist attacks in the aftermath of September 11. Because this bill accomplishes these two goals essential to any effort to modernize FISA, we strongly support passage of this bill and will recommend that the President sign it.
Last August, Congress took an important

step toward modernizing FISA by enacting the Protect America Act of 2007. That Act allowed us temporarily to close intelligence gaps by enabling our intelligence professionals to collect, without having to first obtain a court order, foreign intelligence information from targets overseas. The Act has enabled us to gather significant intelligence critical to protecting our Nation. It has also been implemented in a responsible way, subject to extensive executive, congressional, and judicial oversight in order to protect the country in a manner consistent with safeguarding Americans' civil liberties. Since passage of the Act, the Administration has worked closely with Congress to address the need for long-term FISA modernization. This joint effort has involved compromises on both sides, but we believe that it has resulted in a strong bill that will place the Nation's foreign intelligence effort in this area on a firm, long-term foundation. Below, we have set forth our views on certain important provisions of H.R. 6304.

I. TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE

Title I of H.R. 6304 contains key authorities that would ensure that our intelligence agencies have the tools they need to collect vital foreign intelligence information and would provide significant safeguards for the civil liberties of Americans.

Court Approval. With respect to authorizations for foreign intelligence surveillance directed at foreign targets outside the United States, the bill provides that the Foreign Intelligence Surveillance Court (FISC) would review certifications made by the Attorney General and the Director of National Intelligence relating to these acquisitions, the reasonableness of the procedures used by the Intelligence Community to ensure the targets are overseas, and the minimization procedures used to protect the privacy of Americans. The scope of the FISC's review is carefully and rightly crafted to focus on aspects of the acquisition that may affect the privacy rights of Americans so as not to confer quasi-constitutional rights on foreign terrorists and other foreign intelligence targets outside the United States.

We have been clear that any satisfactory bill could not require individual court orders to target non-United States persons outside the United States, nor could a bill establish a court-approval mechanism that would cause the Intelligence Community to lose valuable foreign intelligence while awaiting such approval, H.R. 6304 would do neither and would retain for the Intelligence Community the speed and agility that it needs to protect the Nation. The bill would establish a schedule for court approval of certifications and procedures relating to renewals of existing acquisition authority. A critical feature of the H.R. 6304 would allow existing acquisitions, which were the subject of court review under the Protect America Act or will be the subject of such review under the H.R. 6304, to continue pending court review. With respect to new acquisitions, absent exigent circumstances. Court review of new procedures and certifications would take place before the Government begins the acquisition. The exigent circumstances exception is critical to allowing the Intelligence Community to respond swiftly to changing circumstances when the Attorney General and the Director of National Intelligence determine that intelligence may be lost or not timely acquired. Such exigent circumstances could arise in certain situations where an unexpected gap has opened in our intelligence collection efforts. Taken together, these provisions would enable the Intelligence Community to keep closed the intelligence gaps that existed before the passage of the Protect America Act and ensure that it will have the opportunity to collect critical foreign intelligence information in the

Exclusive means, H.R. 6304 contains an exclusive means provision that goes beyond the exclusive means provision that was passed as part of FISA. As we have previously stated, we believe that the provision will complicate the ability of Congress to pass, in an emergency situation, a law to authorize immediate collection of communications in the aftermath of an attack or in response to a grave threat to the national security. Unlike other versions of this provision, however, the one in this bill would not restrict the authority of the Government to conduct necessary surveillance for intelligence and law enforcement purposes in a way that would harm national security.

Oversight and Protections for the Civil Liberties of Americans. H.R. 6304 contains numerous provisions that protect the civil liberties of Americans and allow for extensive executive, congressional, and judicial oversight of the use of the authorities. The bill would require the Attorney General and the Director of National Intelligence to conduct semiannual assessments of compliance with targeting procedures and minimization procedures and to submit those assessments to the FISC and to Congress. The FISC and Congress would also receive annual reviews

relating to those acquisitions prepared by the heads of agencies that use the authorities contained in the bill. Congress would receive reviews from the Inspectors General of these agencies and of the Department of Justice regarding compliance with the provisions of the bill. In addition, the bill would require the Attorney General to submit to Congress a report at least semiannually concerning the implementation of the authorities provided by the bill and would expand the categories of FISA-related court documents that the Government must provide to the congressional intelligence and judiciary committees.

Title I also includes provisions that would protect the civil liberties of Americans. For instance, the bill would require for the first time that a court order be obtained to conduct foreign intelligence surveillance outside the United States of an American abroad. Historically, Executive Branch procedures guided the conduct of surveillance of a U.S. person overseas, such as when a U.S. person acts as an agent of a foreign power, e.g., spving on behalf of a foreign government. Given the complexity of extending judicial review to activities outside the United States, these provisions were carefully crafted with Congress to ensure that such review can be accomplished while preserving the necessary flexibility for intelligence operations. Other provisions of the bill address concerns that some voiced about the Protect America Act. such as clarifying that the Government cannot "reverse target" without a court order and requiring that the Attorney General establish guidelines to prevent this from occurring. We believe that, taken together, these provisions will allow for ample oversight of the use of these new authorities and ensure that the privacy and civil liberties of Americans are well protected.

II. TITLE II—PROTECTIONS FOR ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS

Title II of the bill contains, among other provisions, vital protections for electronic communications service providers who assist the Intelligence Community's efforts to protect the Nation from terrorism and other foreign intelligence threats. Title II would provide liability protection related to future assistance while ensuring the protection of sources and methods. Importantly, the bill would also provide the necessary legal protection for those companies who are sued only because they are believed to have helped the Government with communications intelligence activities in the aftermath of September 11, 2001.

The framework contained in the bill for obtaining retroactive liability protection is narrowly tailored. An action must be dismissed if the Attorney General certifies to the district court in which the action is pending that either: (i) the electronic communications service provider did not provide the assistance; or (ii) the assistance was provided in the wake of the September 11 attack and was the subject of a written request or series of requests from a senior Government official indicating that the activity was authorized by the President and determined to be lawful. The district court would be required to review this certification before dismissing the action, and the provision allows for the participation of the parties to the lawsuit in a manner consistent with the protection of classified information. The liability protection provision does not extend to the Government or to Government officials and it does not immunize any criminal conduct.

Providing this liability protection is critical to the Nation's security. As the Senate Select Committee on Intelligence recognized, "the intelligence community cannot

obtain the intelligence it needs without assistance from these companies." That committee also recognized that companies in the future may be less willing to assist the Government if they face the threat of private lawsuits each time they are believed to have provided assistance. Finally, allowing litigation over these matters risks the disclosure of highly classified information regarding intelligence sources and methods. As we have stated on many occasions, it is critical that any long-term FISA modernization legislation contain an effective liability protection provision. H.R. 6304 contains just such a provision and for this reason, as well as those expressed with respect to Title I above, we strongly support its passage.

III. TITLE III—REVIEW OF PREVIOUS ACTIONS

Title III would require the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, and of certain elements of the Intelligence Community to review certain communications surveillance activities, including the Terrorist Surveillance Program described by the President. Although improvements been made over prior versions of this provision, we believe, as we have written before, that it is unnecessary in light of the Inspector General reviews previously completed, those already underway, and the congressional intelligence and judiciary committee oversight already conducted. Nevertheless, we do not believe that, as currently drafted, the provision would create unacceptable operational concerns. The bill contains important provisions to make clear that such reviews should not duplicate reviews already conducted by Inspectors General.

IV. TITLE IV—OTHER PROVISIONS

Title IV contains important provisions that will ensure that the transition between the current authorities and the authorities provided in this bill will not have a detrimental effect on intelligence operations.

Title IV also states that the authorities in the bill sunset at the end of 2012. We have long favored permanent modernization of FISA. The Intelligence Community operates more effectively when the rules governing our intelligence professionals' ability to track our enemies are firmly established. Stability of law also allows the Intelligence Community to invest resources appropriately. Congress has extensively debated and considered the need to modernize FISA since 2006, a process that has involved numerous hearings, briefings, and floor debates. The process has been valuable and necessary, but it has also involved the discussion in open settings of extraordinary information dealing with sensitive intelligence operations. Every time we repeat this process it risks exposing our intelligence sources and methods to our adversaries. Although we would prefer that H.R. 6304 contain no sunset, a sunset in 2012 is significantly longer than others that were proposed and it is long enough to avoid impairing the effectiveness of intelligence operations.

Thank you for the opportunity to present our views on this crucial bill. We reiterate our sincere appreciation to the Congress for working with us on H.R. 6304, a long-term FISA modernization bill that will strengthen the Nation's intelligence capabilities while respecting and protecting the constitutional rights of Americans. We strongly support its prompt passage.

Sincerely,

MICHAEL B. MUKASEY, Attorney General. J.M. McConnell, Director of National Intelligence.

I reserve the balance of my time.

Mr. REYES. Madam Speaker, I yield myself such time as I may consume.

(Mr. REYES asked and was given permission to revise and extend his remarks.)

Mr. REYES. Madam Speaker, I rise today as a sponsor of H.R. 6304, the FISA Amendments Act of 2008. This bill represents the culmination of more than a year's work by the members and staff of the House Intelligence Committee, together with our colleagues on the Judiciary Committee, to bring to the floor a bill that modernizes our surveillance authorities while protecting the constitutional rights of Americans.

I want to thank Chairman Conyers for his efforts to strengthen this bill. As always, I greatly appreciate my good friend's commitment to protecting our country and the principles that we hold so dear. I also want to thank the respective ranking members and all that worked so hard to bring

this bill to the floor today.

This bill, Madam Speaker, enjoys wide support inside the Democratic Caucus. It has been endorsed by our Democratic whip, by our Democratic Caucus chair, by the Blue Dog Coalition, the New Democratic Caucus and by a number of our colleagues. For that, I want to thank in particular our majority leader, Mr. HOYER, for leading the effort towards a bipartisan compromise. This bill is a far better deal than the Protect America Act. And it is far better than the Senate bill that passed earlier this year.

Madam Speaker, intelligence is the first line of defense in our Nation's effort to prevent terrorism and to stop the proliferation of weapons of mass destruction. This legislation strengthens the ability of our intelligence agencies to conduct lawful surveillance of foreign targets. But this legislation also serves another very important and vital function. It strengthens the constitutional rights of Americans, protects them from unlawful surveillance and it stops this President, or any President, for that matter, from invokexecutive power to conduct warrantless surveillance of Americans.

□ 1100

This bill does more than just retain the original FISA requirements for an individual warrant based upon probable cause for surveillance targeting Americans here in the United States. For the first time ever, this bill requires in statute warrants for Americans anywhere in the world. It also requires the government to establish clear guidelines to ensure that no American is the target of any surveillance without a warrant. It clarifies that FISA and Title 18, the Criminal Code, are the exclusive means by which the government may conduct domestic surveillance.

It will prohibit any unlawful, warrantless wiretapping, the kind we saw under this administration. It provides accountability by requiring the inspectors general of various agencies to compile a comprehensive report on the President's surveillance program

and that review must be given to Congress. It requires prior court approval of the procedures used to conduct surveillance of foreign targets, except in an emergency, similar to the current FTSA law.

This legislation, Madam Speaker, also addresses the issue of lawsuits against telecommunications companies that comply with directives from our government. This bill does not grant immunity to any government official who might have violated the law, and this bill does not grant automatic immunity to telecom companies, as the Senate bill would have.

Under this legislation, a Federal District Court will review the evidence

submitted by the Attorney General and then the court will decide whether to grant civil liability and protection to a company that provided post-9/11 assistance to the government. This bill does not grant immunity. Congress isn't deciding the question of immunity; the District Court will.

Finally, Madam Speaker, this bill will sunset in 4½ years, ensuring that the next administration will be in a position to assess and review the effectiveness of this legislation.

This legislation represents a bipartisan compromise, and, as such, both sides got less than they wanted. But it is a product of a good faith effort by both Republicans and Democrats to give our intelligence agencies the tools necessary to keep America safe, while protecting our Constitution and our civil liberties.

I strongly urge my colleagues to vote for this very important piece of legisla-

In addition, Chairman REYES submitted the following views for the RECORD:

EXIGENT CIRCUMSTANCES

Prior court review is an absolutely integral part of this bill, but we have also crafted an "exigent circumstances" circumstances provision that allows the Administration to commence surveillance immediately in an emergency. This provision should be invoked rarely, if at all. In the normal course of events, the Attorney General and the Director of National Intelligence will have ample time to submit applications for surveillance to the FISA Court for its approval before initiating a particular surveillance.

When used, this exception should be for purposes of a true emergency, involving unforeseen or extraordinary circumstances. I consider this to be limited to situations where the intelligence sought would serve a critical function in protecting national security and where the failure to act immediately would result in the loss of what might be the only opportunity to collect the information in question.

The Intelligence Committee intends to engage in regular and vigorous oversight of these new authorities and, in particular, the use of the "exigent circumstances" exception to ensure that the important protections in this bill are not circumvented.

"REVERSE TARGETING"

The FISA Amendments Act of 2008 regularly uses the term "targeting." We intend this term to mean more than simply the process of selecting a telephone number of an e-mail address to surveil. Rather, it is meant to describe the process of purposely acquiring communications of or information about a specific individual.

It is in this context that Section 702(b)(2) prohibits what is generally referred to as "reverse targeting." In our discussions with the intelligence agencies, they have agreed that this language prohibits the targeting of one or more persons overseas where the purpose is to acquire the communications of or information about a U.S. person or any specific person reasonably believed to be inside the United States. Accordingly, Section 702(f) requires that the government adopt guidelines to ensure that this does not occur.

$\begin{array}{c} \text{INADVERTENT COLLECTION OF U.s.-PERSON} \\ \text{INFORMATION} \end{array}$

Because of the nature of the new surveillance authorities granted under this bill, we were particularly concerned about the potential for a significant increase in the inadvertent collection of U.S.-person communications and information. For that reason, we have adopted several oversight provisions that require the Intelligence Community to report to Congress on the number of targets later determined to have been located inside the United States, the number of disseminated intelligence reports that contain U.S.person information, and the number of disseminated intelligence reports that contain information identifying specific U.S. persons. The Intelligence Committee plans to conduct vigorous oversight of the reports.

EXCLUSIVITY

The exclusivity provision of this bill is extremely important. This language is designed to prevent any future efforts to conduct surveillance that is not authorized by statute. The bill not only establishes that FISA and Title 18 are the exclusive means of conducting surveillance, it requires that any future authorization for surveillance must be explicitly established in statute. The language should in no way be read to imply that there is an inherent power to conduct surveillance beyond what is expressly authorized by statute.

In particular, the language in Section 102(c)(1)(ii) should be read to require citation to specific statutory authority in all certifications for assistance in conducting electronic surveillance issued pursuant to 18 U.S.C. §2511(2)(a)(ii)(B).

SUNSET

This bill is set to expire on December 31, 2012. During the next four years, Congress will continue to assess the surveillance activities of the U.S. Government and assess whether additional changes need to enacted before the sunset date to correct any deficiencies or problems that arise.

CIVIL LIABILITY PROVISIONS

The provisions in title II of this bill establish a meaningful court review to determine whether telecommunications companies should be protected from civil liability for assistance provided to the government. It is important to state that these provisions are not intended to imply in any way that the President's conduct in connection with the President's warrantless surveillance program was lawful or to excuse the conduct of any government official that might have violated the law.

Further, no telecommunications company should interpret these provisions to imply that Congress will act in the future to seek the dismissal of any other lawsuits charging improper conduct in connection with surveillance activities. Rather, Congress considers the tragic events of 9/11 to be a unique set of circumstances that require special consideration. As a general matter, we expect companies and private citizens to respect the rule of law and to require the same of its government.

With respect to the applicable legal standard, we intend "substantial evidence" to apply not only to a finding that assistance was provided in response to a request that

meets the standard of this bill. That standard should also apply where the court is asked to determine that the alleged assistance was not provided. A simple declaration from the Government or the defendant that the alleged assistance did not occur should be deemed insufficient where there is sufficient evidence to the contrary.

Similarly, when the Government alleges that a surveillance program was "designed" (as opposed to "intended") to detect and prevent terrorism, the court should examine the evidence to assess the scope of the program and determine, where appropriate, that indiscriminate surveillance that acquires the communications of millions of Americans is not truly "designed" to detect or prevent terrorism.

Finally, these provisions should also not be interpreted to remove the power of the courts to review the constitutionality of the process this bill establishes.

Mr. REYES. Madam Speaker, I reserve the balance of my time.

Mr. HOEKSTRA. Madam Speaker, I yield 3 minutes to the gentleman from Missouri (Mr. Blunt), the distinguished minority whip, who played such a critical role in ensuring that this bill made it to the floor today.

Mr. BLUNT. Madam Speaker, I thank Mr. Hoekstra for yielding me this initial time that would have the other-

wise gone to you.

I thank you, Mr. HOEKSTRA, Mr. REYES and Mr. SMITH, for bringing this important piece of legislation to the floor and for working so hard to see that it came to the floor. I would also like to say that I again appreciated the opportunity to work with my good friend Mr. HOYER, as he spent so many hours and so much time on this. From his staff, Mariah Sixkiller; from my staff, Brian Diffel: Mr. BOEHNER's staff. Jen Stewart worked hard on this; Chris Donesa from Mr. Hoekstra's staff was indispensable in his work, as was Caroline Lynch from Mr. SMITH's staff. And I got to know frankly and work with Jeremy Bash from Mr. REYES' staff and Lou DeBaca from Mr. Conyers' staff, and appreciated the real positive contributions they bring to this process every day.

I would also like to suggest that two staffers of my colleague from Missouri, Mr. BOND, Louis Tucker, and Jack Livingston, spent lots of time and lots of productive work on this.

Madam Speaker, this represents a compromise, as Mr. Reyes just said, as Mr. Smith just said, that was forged with lots of hard work by lots of people. It accomplishes the goals of the intelligence community. There is no individualized court order for targeting foreign terrorists in foreign countries. There are protections here for communications providers that may have assisted the government. But, as Mr. Reyes just said, those protections will be determined by a court, not by this legislation

We modernized the law to adapt to changes in technology since the 1978 FISA statute. The bill would accomplish all this while adding new protections and strengthening the individual liberties and privacy protections of Americans.

We also worked closely with the majority to reinforce the FISA Court's role in procedural certifications and reviews of administration policies, and we created some new obligations for the Attorney General to establish guidelines.

Madam Speaker, like yesterday's vote, this bill is an example of what we can do when we work together. I thank all those who worked so hard to get it to the floor today. I urge my colleagues to vote for it.

Mr. CONYERS. Madam Speaker, is it true that I have 10 minutes remaining?

The SPEAKER pro tempore. The gentleman from Michigan has 10½ minutes remaining.

Mr. CONYERS. I am going to recognize Mr. NADLER, Ms. LOFGREN, Mr. SCOTT, Ms. JACKSON-LEE, Mr. HOLT, Ms. LEE, Mr. CAPUANO, Mr. KUCINICH and Mr. INSLEE. A couple of them will get $1\frac{1}{2}$ minutes.

The first one to be recognized is the chairman of the Crime Subcommittee, the gentleman from Virginia (Mr. SCOTT), for 1½ minutes.

Mr. SCOTT of Virginia. Madam Speaker, I oppose H.R. 6304. It allows widespread acquisition of private conversations without meaningful court review. The bill actually permits the government to perform mass untargeted surveillance of any and all conversations believed to be coming into and out of the United States without any individualized finding and without a requirement that wrongdoing is believed to be involved at all.

It arguably is not limited just to terrorism. It could be any foreign intelligence, which would include diplomacy and anything else. It is vague on what can be done with the information after it is acquired and who has access to it, and the only court review is a check on whether or not the government certifies that the process has been followed. The court does not review who, what and where the tapping will take place.

Furthermore, the collection of all of this data can be done under emergency provisions before the court acts, but the collection can continue to be done even if the court later rejects the application if the administration appeals.

The bill also provides retroactive immunity to communications companies who may have violated people's rights, and whether or not those rights have been violated should be reviewed by the courts, not decided here in Congress.

Madam Speaker, we can protect Americans' national security and protect civil rights by providing government access to personal conversations with meaningful court review. This bill fails to do that, and therefore should be defeated

Mr. SMITH of Texas. Madam Speaker, I yield 1 minute to the gentleman from Virginia (Mr. FORBES), a member of the Judiciary Committee and the Armed Services Committee.

Mr. FORBES. Madam Speaker, today when the sun comes up on America,

there are all too many people who spend all too much time criticizing and apologizing for this Nation, trying to verbally tear it down. But what frightens us most is those people who spend way too much energy and way too much time trying to do harm to innocent Americans as they go about their day-to-day lives, carrying their children to piano recitals, to Little League practice, just going to work. It just makes common sense that we would want to know what they were trying to do, because if we know, we have at least a chance to stop it.

This is a bipartisan bill that we should have had a year ago. We certainly should have had 4 months ago. Thank goodness we have it today. The only unfortunate thing is those who will benefit the most will never know it, because they never became victims because we were able to stop those terrorist acts before they took place.

Mr. REYES. Madam Speaker, I yield 1 minute to the distinguished gentleman from Missouri (Mr. Skelton), the chairman of the Armed Services Committee.

Mr. SKELTON. Madam Speaker, today I rise in strong support of this bill, the FISA Amendments Act of 2008. The bipartisan compromise before us strikes the right balance between providing our intelligence community with the tools they need to fight and find terrorists and protecting our constitutional rights on the other hand.

Let me thank my colleagues SYL-VESTER REYES and JOHN CONYERS, our Intelligence and Judiciary Committee chairmen, for their hard work. I am pleased that we have resolved this critical national security issue through bipartisan negotiations between the administration and the Congress. I want to particularly commend STENY HOYER, our majority leader, and our Speaker, NANCY PELOSI, for their leadership in reaching this landmark legislation.

The bill before us is a great improvement over the Senate bill in that it provides for more rigorous review of electronic surveillance activities. It gives the courts a meaningful role in determining if telecommunication firms are entitled to civil liability protection.

The SPEAKER pro tempore. The time of the gentleman has expired.

Mr. REYES. I grant the gentleman an additional 30 seconds.

Mr. SKELTON. From my perspective as chairman of the Armed Services Committee, the bill strongly supports the intelligence needs of those who wear the uniform. Every day, American men and women deployed in harm's way depend on electronic surveillance capabilities to achieve their missions. Because of this bill and the work that has been done in this Congress, especially the Intelligence Committee and the Judiciary Committee, I thank them, and at the end of the day the young men and young women will be the beneficiaries of this strong legisla-

Madam Speaker, I rise today in strong support of H.R. 6304, the FISA Amendments Act of 2008.

The bipartisan compromise before us today strikes the right balance between providing our intelligence community with the tools they need to find and fight terrorists, and protecting our constitutional rights.

I want to thank my colleagues, SILVESTRE REYES and JOHN CONYERS, our Intelligence and Judiciary Committee Chairmen, for their hard work in bringing a strong bill to the floor today.

I am pleased that we have resolved this critical national security issue through bipartisan negotiations between the Administration and the Congress and I want to particularly commend Speaker NANCY PELOSI and STENY HOYER for their leadership in reaching this landmark legislation.

The bill before us today is a great improvement over the Senate bill in that it provides for more rigorous review of electronic surveillance activities, and gives the courts a meaningful role in determining if telecommunications firms are entitled to civil liability protection.

From my perspective, as the Chairman of the Armed Services Committee, this bill strongly supports the intelligence needs of our soldiers, sailors, airmen and marines. Every day, American men and women deployed in harm's way depend on the electronic surveillance capabilities to achieve their missions. This legislation ensures continued delivery of this intelligence to our warfighters.

Again, I want to congratulate Chairman REYES and Chairman CONYERS or bringing this strong bill to the floor, and I urge my colleagues to join me in supporting this vital na-

tional security measure.

Mr. HOEKSTRA. Madam Speaker, I vield 2 minutes to the distinguished member of the Intelligence Committee from Texas (Mr. THORNBERRY).

Mr. THORNBERRY. Madam Speaker, the compromise bill before us today is not the bill that I would have written. As a matter of fact, the compromise Senate bill we have been trying to get a vote on since February is not the bill I would have written either. But I do believe that the bill before us, imperfect as it is, does do what is needed to protect the country, and therefore I

support it.

A number of people deserve credit. including Mr. Hoekstra, Mr. Blunt and Mrs. Wilson on our side. But I also want to commend the majority leader, Mr. HOYER, for the time and energy he put into this issue and for his perseverance in pushing it to a resolution. I know a number of Members on his side don't want to do anything. They prefer operating under an outdated law that makes it impossible to move with the speed and agility we need to have to protect the country in an age of terrorism. There may be some on this side who would prefer to have a political issue for the fall campaign.

But I believe that every day we grow more vulnerable, and that we must act now to give our national security professionals, including our troops in the field, the tools and the information they need to do their job.

Madam Speaker, the House has taken some significant steps this week to-

ward ending the disturbing practice of playing politics with national security. When this House is allowed to vote, we can come together and accomplish things for the country. If we can just extend that now into energy and other issues and just allow a vote on the proposals that are before us, we can do good for the country in other areas as

Mr. CONYERS. Madam Speaker, I yield 1½ minutes to the gentlewoman from California (Ms. ZOE LOFGREN), the Chair of the Immigration committee.

Ms. ZOE LOFGREN of California. Madam Speaker, I rise in opposition to this bill. I appreciate that some improvements have made been made to title I of the bill, but even these improvements are undercut by the scheme in title II that means there will be no accountability and perhaps no adherence to the provisions of title I.

I cannot support the legislation's deeply flawed provisions relating to the issue of immunity for telecommunications companies. These provisions turn the judiciary into the administration's rubber stamp. The review provided in this bill is an empty formality that will lead to a preordained conclusion, dismissing all cases with no examination on their merits.

Under this bill, the courts are not allowed to ask whether the conduct of the corporations who assisted was in fact legal. They may only note that the administration says that it was legal. In other words, the decision on the ultimate question of legality, a decision the Constitution dedicates to the judiciary, will instead be made by the executive branch with the judiciary acting as a rubber stamp. It turns the process of judicial review into a joke and denigrates this supposedly independent and coequal branch of government.

□ 1115

It's all the more aggravating because immunity already exists in the law under 18 U.S.C., section 2511. It provides that telecommunications companies are immune from suit if the company has been provided with a court order or a certification by the Attorney General, in writing, that the order has been obtained or is unnecessary.

I cannot support this.

(Effective: November 25, 2002) UNITED STATES CODE ANNOTATED CURRENTNESS

Title 18. Crimes and Criminal Procedure (Refs & Annos)

Part I. Crimes (Refs & Annos)

Chapter 119. Wire and Electronic Communications Interception and Interception of Oral Communications (Refs & Annos)

§2511. Interception and disclosure of wire, oral, or electronic communications prohibited

- (1) Except as otherwise specifically provided in this chapter any person who-
- (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
- (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor

to use any electronic, mechanical, or other device to intercept any oral communication

- (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
- (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
- (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce: or
- (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
- (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States:
- (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection: or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or

other specified person, has been provided

(A) a court order directing such assistance

signed by the authorizing judge, or (B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications

system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person-

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted-

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public:

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which-

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider. another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer,

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer:

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication-

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or an addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agen-

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted-

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public. but not including data transmissions or telephone calls.

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

[(c) Redesignated (b)]

(5)(a)(i) If the communication is-

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdic-

(ii) In an action under this subsection-

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief: and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory \$500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than \$500 for each violation of such an injunction.

Mr. SMITH of Texas. Madam Speaker, I will yield 2 minutes to the gentleman from Indiana (Mr. Pence) who is a member of the Judiciary Committee and the Foreign Affairs Committee as well.

(Mr. PENCE asked and was given permission to revise and extend his remarks)

Mr. PENCE. Madam Speaker, I rise in support of the FISA Amendments Act of 2008.

America is at war. We have to do all we can to protect our Nation from those who seek to harm this country, our communities and our families.

After nearly a year of delays, we finally have before us a bill that will institute a long-term fix to our Nation's foreign intelligence surveillance laws and provide the intelligence community with the tools it needs to protect this country.

I rise in particular appreciation of Republican Whip Roy Blunt, Ranking Member Smith and Mr. Hoekstra. These Republicans stood firm and have succeeded in negotiating a strong 4-year extension to our surveillance laws.

While this bill is tough on terrorists, it includes strong protections for civil liberties and Americans that have also been put in place by extensive measures of oversight and review in the Department of Justice, and it protects those patriotic telecommunications companies who assisted the Federal Government in the wake of 9/11.

While I endorse these reforms and safeguards, let me say, Madam Speaker, Congress and future administrations must be vigilant to ensure that the exigent circumstances exceptions are practiced in a way that preserves Presidential discretion when conducting real-time foreign intelligence. Speaking less as a Congressman and more as a father, and as an American who was here on September 11, I am grateful to my colleagues in both parties for bringing this important compromise to the floor and making sure that our intelligence community, those who work tirelessly every day to protect us, have the tools they need to prevent the horrors of that day from ever being visited on our soil again.

Mr. REYES. Madam Speaker, I yield 2 minutes to the distinguished gentle-woman from California, Ms. JANE HARMAN, who is the former ranking member of the Intelligence Committee.

(Ms. HARMAN asked and was given permission to revise and extend her remarks.)

Ms. HARMAN. Madam Speaker, my phones are ringing off the hook, and my e-mail accounts are full. By the hundreds and hundreds, my constituents are saying, "don't cave in," "don't toss due process out the window," "no compromise on our civil liberties" and "all surveillance of Americans should require a warrant." One of the most powerful, "The U.S. Constitution has been 'marked up.' Don't shred it."

I agree, now and always. The hard part is deciding whether the FISA compromise before us meets my constituents' requirements and my own.

After reading every word of it, and after many, many hours working to develop and revise portions of it, I conclude that the compromise replaces bad law, the Protect America Act, with law that actually improves many of the provisions of the underlying FISA law which has served our country well for three decades.

Let me highlight three issues.

First, this bill makes clear that no president can ignore it ever again. FISA is the exclusive means by which our government can conduct surveillance. In short, no more warrantless surveillance.

Second, it expands the circumstances for which individual warrants are required, by including Americans outside the U.S., and it protects Americans from so-called reverse targeting.

Third, it requires Federal court review to determine whether communications firms, which assisted in post-9/11 activities, get civil liability protection. If the evidence is inadequate, courts can deny immunity, and immunity does not cover government officials who may have violated the law.

I have lived with FISA up close and personal for many years. I am angry about the way the Bush administration abused it and disrespected Congress. My constituents are right to demand that Congress show courage and stand up for the Constitution. Security and liberty are reinforcing values, not a zero-sum gain. This bill, though imperfect, protects both.

Mr. SMITH of Texas. Madam Speaker, I yield 1 minute to the gentleman from Ohio (Mr. BOEHNER) who is the distinguished Republican leader of the House.

Mr. BOEHNER. Let me thank my colleague from Texas for yielding.

Let me just take a moment to congratulate both Mr. SMITH, ranking member on the Judiciary Committee, and Mr. HOEKSTRA, the ranking member on the Intelligence Committee, and all of their staff, who have worked closely with our Democrat colleagues, both in the House and Senate, to craft a bill that will help protect the American people.

Madam Speaker, America cannot afford to have a pre-9/11 mentality when it comes to national security. I think that's why this bill is so critical and why Members and staff have been working so hard to craft it. I recognize the serious threat that we face, and it keeps our Nation on offense when it comes to protecting the American people.

Our intelligence officials must have the ability to monitor terrorists suspected of plotting to kill Americans. This measure ensures that the tools that they need will be there to help keep America safe. They have retroactive liability protections for firms that have aided the government and have worked with our government at our request to help detect and prevent attacks. We should protect those companies.

I think it also protects the civil liberties of all Americans. This is an important piece of legislation. It has taken an awful lot of time to get there.

But just like yesterday, when Members on both sides of the aisle work together, we can come to an agreement. We can come to a compromise that's in the best interest of our country.

Two days in a row we have had two great examples of how we can craft very good bills by working in a bipartisan manner. I want to congratulate all the Members on both sides of the aisle and their staffs who have worked so hard to bring this bill to the floor.

Mr. CONYERS. Madam Speaker, I would like now to yield to the chairman of the subcommittee on the Constitution and the Judiciary, the gentleman from New York, Jerry Nadler, 1½ minutes.

Mr. NADLER. Madam Speaker, in order to uphold the principle of the rule of law and the supremacy of the Constitution, we must reject this bill. This bill limits the courts hearing lawsuits alleging illegal wiretapping, to considering only whether the telecom companies received a "written request or directive indicating that the activity was authorized by the President and determined to be lawful," not whether that request was actually lawful or that telecom companies knew that it was unlawful.

The bill is a fig leaf granting blanket immunity to the telecom companies for possibly illegal acts without allowing the courts to consider the facts or the law. It denies people whose rights are violated their fair day in court, and it denies the American people the right to have the actions of this administration subjected to fair and independent scrutiny.

Even the court's limited review will remain secret. The lawsuits will be dismissed, but the basis for that dismissal that the defendants were innocent of misconduct or that they were guilty, but that Congress commands their immunity, must remain secret.

The constitutionality of the immunity granted by this bill is very questionable. As Judge Walker put it in the AT&T case, "AT&T's alleged actions here violate the constitutional rights clearly established in the Keith decision. Moreover, because the very action in question has previously been held unlawful, AT&T cannot seriously contend that a reasonable entity in its position could have believed that the alleged domestic dragnet was legal."

I would hope that the courts will find that because the constitutional rights of Americans have been violated, Congress' attempt to prevent court review is unconstitutional. I regret we may today abandon the Constitution's protections and insulate lawless behavior from legal scrutiny.

I urge a "no" vote on this legislation.

Mr. HOEKSTRA. Madam Speaker, at this time I would like to yield 3 minutes to a member of the committee, Mrs. WILSON from New Mexico.

(Mrs. WILSON of New Mexico asked and was given permission to revise and extend her remarks.)

Mrs. WILSON of New Mexico. Madam Speaker, in December of 2005, I was walking to work and was at 1st and C Street when the front page of the New York Times revealed the existence of a program that had not been previously briefed to the entire Intelligence Committee and to the subcommittee that I, at that time, chaired that oversaw the activities of the National Security Agency. That launched a period of extensive oversight and draft legislation in 2006.

In January of 2007, because legislation didn't pass, the administration made an attempt to put this entire program under a FISA law that was not designed and was not updated. I described that at the time as trying to put a twin-size sheet on a king-size bed. It didn't work.

By late summer of 2007, we had lost close to two-thirds of our intelligence collection on terrorism. We were unable to respond fast enough when we had problems, particularly in war zones.

Just before Memorial Day in 2007, we had three soldiers who were kidnapped in Iraq. We needed an Army of lawyers in Washington D.C. to listen to the communications of the people that we thought had kidnapped them.

That delay is not good enough and led to the insistence that we pass the Protect America Act, which this Congress did, over the objections of the Democratic leadership, in August of 2007. The Protect America Act closed an important intelligence gap, but it expired in February of this year, and the gap is at risk of ever widening.

The bill that we pass today will protect the civil liberties of Americans and continue to require individualized warrants for anyone in the United States or American citizens anywhere in the world. It will also allow our intelligence agencies to very rapidly follow up on tips and listen to foreigners in foreign countries who are trying to kill Americans.

We have restored FISA to its original intent and modernized it for 21st century communications and technology. This is an important step for our intelligence community and will put it on a sound footing for the next several decades.

Intelligence, good intelligence, is the first line of defense against terrorism, and today this body will take the next step in making sure we have the tools to be able to listen to our enemies and prevent other terrorist attacks.

I would urge my colleagues to support the legislation.

Mr. CONYERS. Madam Speaker, I would like to yield now to a senior member of Judiciary, Sheila Jackson-Lee of Texas, 1 minute.

Ms. JACKSON-LEE of Texas. I thank the distinguished chairman.

Madam Speaker, I rise to say that we did have legislation that would protect the Constitution and provide the security for our troops and those in the intelligence community, and that was the RESTORE Act. Today I rise in enormous opposition to H.R. 6304 because, frankly, Madam Speaker, it's very difficult to put lipstick on a pig.

What we have here is the opportunity for the government to conduct mass, untargeted surveillance of all communications coming into and out of the United States without any individual review and without any finding of wrongdoing.

What Americans don't know is that this government can now surveil you for 7 days without any approval. Then if the court denies the application, while the application is being appealed from the denial, you can be surveilled for 60 days.

This is not constitutional protection. As it relates to the idea of those who are now in court on warrantless searches, now the courts have no authority over that, and your cases will be dismissed.

I ask my colleagues to oppose this because "significant purpose" has been taken out of this legislation.

Madam Speaker, I rise today in opposition to H.R. 6304, the "FISA Amendments Act of 2008". This body has worked diligently with our colleagues in the Senate to ensure that the civil liberties of American citizens are appropriately addressed. Sadly, this compromise bill falls short of that aim. I will support no bill that fails to protect American civil liberties, both at home and abroad.

I am unable to support this bill that will overhaul how the Government monitors foreign terrorist suspects. I will not support any legislation that grants legal immunity to telecommunications companies that provide information to Federal investigators without a warrant.

Madam Speaker, this administration has the law to protect the American people. When Americans are involved, the Bill of Rights, the fourth amendment, and our civil liberties must be adhered to. This legislation does not go far enough to ensure that American rights are protected.

The original legislation offered by the House Majority gave the Administration everything that it needed, but today, after months of negotiation, if we endorse H.R. 6304, which grants sweeping wiretapping authority to the Government with little court oversight and ensures the dismissal of all pending cases against the telecommunications companies, we are eviscerating the Constitution.

Let me explain my objections to H.R. 6304. It permits the Government to conduct mass, untargeted surveillance of all communications coming into and out of the United States, without any individualized review, and without any finding of wrongdoing.

H.R. 6304 permits minimal court oversight. The Foreign Intelligence Surveillance Court (FISA Court) only reviews general procedures for targeting and minimizing the use of information that is collected. Under these circumstances, the court may not know what will be tapped and where it will occur.

Furthermore, the bill contains a general ban on reverse targeting, but not the strong language I worked so diligently to include in the FISA legislation that had passed previously in the House. In my view, the RESTORE Act is far superior to this piece of legislation. I wish to take a few moments to discuss the improvement that I offered to the RESTORE Act in the full Judiciary Committee markup, and which was sent over to the Senate for consideration last year.

My amendment made an essential contribution to the RESTORE Act by laying down a clear, objective criterion for the administration to follow and the FISA court to enforce in preventing reverse targeting.

Reverse targeting is the practice where the Government targets foreigners without a warrant while its actual purpose is to collect information on certain U.S. persons. My language included clear statutory directives regarding whom the government should return to the FISA court and obtain an individualized order if it would like to continue listening to an Americans' communications.

One of the major concerns that libertarians and classical conservatives, as well as progressives and civil liberties organizations, have with this legislation, as they did with its successor, the Protect America Act, is that the temptation of national security agencies to engage in reverse targeting may be difficult to resist in the absence of certain safeguards in the law to prevent it.

My amendment attempted to produce such safeguards. My amendment reduced even further any such temptation to resort to reverse targeting by requiring the administration to obtain a regular, individualized FISA warrant whenever the "real" target of the surveillance is a person in the United States.

The amendment achieved this objective by requiring the administration to obtain a regular FISA warrant whenever a "significant purpose of an acquisition is to acquire the communications of a specific person reasonably believed to be located in the United States."

It is far from clear how the operative language "reasonably designed to ensure that any acquisition authorized . . . is limited to targeting persons reasonably believed to be located outside the United States; and prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States."

Yes. It is true that H.R. 6304, the compromise legislation, attempts to ensure that American civil liberties are protected, but the operative language in the legislation does not provide a paradigm for consistency. This is so because it does not provide an objective criterion. H.R. 6304 does not go as far as the legislation that the House sent over to the Senate a few months ago. H.R. 6304 does not retain the objective standards contained in my amendment.

The language used in my amendment, "significant purpose," is a term of art that long has been a staple of FISA jurisprudence and thus is well known and readily applied by agencies, legal practitioners, and the FISA Court. Thus, the Jackson-Lee amendment provided a clearer, more objective criterion for the administration to follow and the FISA court to enforce to prevent the practice of reverse targeting without a warrant, which all of us can agree should not be permitted.

A FISA order should be required in those instances where there is a particular, known person in the United States at the other end of the foreign target's call in whom the Government has a significant interest such that a significant purpose of the surveillance has become to acquire that person's communications. This protection has been stripped from H.R. 6304. I fought hard to keep this language in the bill because it is important to me; and it should be very important to members of this body and to all Americans. It is important that we require what should be required in all cases—warrant any time there is specific, targeted surveillance of a United States citizen.

Madam Speaker, I have more objections to H.R. 6304 which I will quickly note. H.R. 6304 contains an "exigent" circumstances loophole that thwarts the judicial review requirement. The bill permits the Government to start a spying program and wait to go to court for up to seven (7) days every time "intelligence important to the national security of the U.S. may be lost or not timely acquired." The problem with H.R. 6034 is that court applications take time and will delay the collection of information. Therefore, it is possible that there will not be resort to prior judicial review.

Under H.R. 6304, the Government is permitted to continue surveillance programs even if the application is denied by the court. The Government has the authority to wiretap through the entire appeals process, and then keep and use whatever it gathers in the meantime.

I am also troubled by H.R. 6304's dismissal of all cases pending against telecommunication companies that facilitated the warrantless wiretapping program over the last 7 years. The test in the bill is not whether the Government certifications were actually legal—only whether they were issued. Because it is public knowledge that they were, all the cases seeking to find out what these companies and the Government did without communications will be dismissed. Under this bill, we will start as a tabula rasa. Telecommunications companies will be prevented from having their day in court and we, the American people, will never have a chance to know what the companies did and what information is collected. I am deeply troubled by this, and frankly, you should be, too.

Madam Speaker, it is important to point out that the loudest demands for blanket immunity did not come from the telecommunications companies but from the administration, which raises the interesting question of whether the administration's real motivation is to shield from public disclosure the ways and means by which Government officials may have "persuaded" telecommunications companies to assist in its warrantless surveillance programs.

Madam Speaker, let me be clear in my opposition. Nothing in the Act or the amendments to the Act should require the Government to obtain a FISA order for every overseas target on the off chance that they might pick up a call into or from the United States. Rather, what should be required, is a FISA order only where there is a particular, known person in the United States at the other end of the foreign target's calls in whom the Government has a significant interest such that a significant purpose of the surveillance has become to acquire that person's communications.

Nearly two centuries ago, Alexis de Tocqueville, who remains the most astute stu-

dent of American democracy, observed that the reason democracies invariably prevail in any martial conflict is because democracy is the governmental form that best rewards and encourages those traits that are indispensable to martial success: initiative, innovation, resourcefulness, and courage.

As I wrote in the Politico, "the best way to win the war on terror is to remain true to our democratic traditions. If it retains its democratic character, no nation and no loose confederation of international villains will defeat the United States in the pursuit of its vital interests."

Thus, the way forward to victory in the war on terror is for the United States country to redouble its commitment to the Bill of Rights and the democratic values which every American will risk his or her life to defend. It is only by preserving our attachment to these cherished values that America will remain forever the home of the free, the land of the brave, and the country we love.

Madam Speaker, FISA has served the Nation well for nearly 30 years, placing electronic surveillance inside the United States for foreign intelligence and counterintelligence purposes on a sound legal footing, and I am far from persuaded that it needs to be jettisoned.

However, I know that FISA as outlined in this bill, H.R. 6304, attempts to curtail the Bill of Rights and the civil liberties of the American people. I continue to insist upon individual warrants, based upon probable cause, when surveillance is directed at people in the United States. The Attorney General must still be required to submit procedures for international surveillance to the Foreign Intelligence Surveillance Court for approval, but the FISA Court should not be allowed to issue a "basket warrant" without making individual determinations about foreign surveillance.

In all candor, Madam Speaker, I must restate my firm conviction that when it comes to the track record of this President's warrantless surveillance programs, there is still not enough on the public record about the nature and effectiveness of those programs, or the trust-worthiness of this administration, to indicate that they require a blank check from Congress.

The Bush administration did not comply with its legal obligation under the National Security Act of 1947 to keep the Intelligence Committees "fully and currently informed" of U.S. intelligence activities. Congress cannot continue to rely on incomplete information from the Bush administration or revelations in the media. It must conduct a full and complete inquiry into electronic surveillance in the United States and related domestic activities of the NSA, both those that occur within FISA and those that occur outside FISA.

The inquiry must not be limited to the legal questions. It must include the operational details of each program of intelligence surveillance within the United States, including: (1) who the NSA is targeting; (2) how it identifies its targets; (3) the information the program collects and disseminates; and most important (4) whether the program advances national security interests without unduly compromising the privacy rights of the American people.

Given the unprecedented amount of information Americans now transmit electronically and the post-9/11 loosening of regulations governing information sharing, the risk of intercepting and disseminating the communications

of ordinary Americans is vastly increased, requiring more precise—not looser—standards, closer oversight, new mechanisms for minimization, and limits on retention of inadvertently intercepted communications.

Madam Speaker, I encourage my colleagues to join me in opposition to H.R. 6304, as it grants sweeping wiretapping authority to the Government with little court oversight and ensures the dismissal of all pending cases against the telecommunications companies. In my view, this is wrong and unacceptable.

Mr. SMITH of Texas. Madam Speak-

Mr. SMITH of Texas. Madam Speaker, I yield 1 minute to the gentleman from Arizona (Mr. Franks) who is a member of the Judiciary Committee and a ranking member of the Constitution Subcommittee.

□ 1130

Mr. FRANKS of Arizona. I thank the gentleman for yielding me this time.

Madam Speaker, the coincidence of jihadist terrorism and nuclear proliferation in our world today I believe represents the greatest security threat to the human family. Osama bin Laden said "our religious duty is to gain nuclear weapons." If that quest should succeed, whether it is 100 yards from this Capitol or in one of our major cities, it will change our concept of freedom in a way that almost none of us can comprehend. And our best hope of preventing that is to have effective intelligence capability.

I believe that the majority has risked the security of this country by delaying a vote on this important bill for so long; but I am gratified today that at least we are taking the next step in making sure that we can see our children and grandchildren walk in the sunlight of freedom.

As we go forward, we should all keep in mind the words of our Founding Fathers and the words especially of Thomas Jefferson when he said, "The price of freedom is eternal vigilance."

Mr. REYES. Madam Speaker, may I inquire as to how much time remains on all sides.

The SPEAKER pro tempore. The gentleman from Michigan (Mr. CONYERS) has 5 minutes remaining; the gentleman from Texas (Mr. REYES) has 6½ minutes remaining; the gentleman from Texas (Mr. SMITH) has 8 minutes remaining; and the gentleman from Michigan (Mr. HOEKSTRA) has 7½ minutes remaining.

Mr. REYES. Madam Speaker, I now would like to yield 2 minutes to the distinguished gentleman from Maryland (Mr. RUPPERSBERGER) who serves as the chairman of our Subcommittee on Technical and Tactical Intelligence on our Intelligence Committee.

Mr. RUPPERSBERGER. Madam Speaker, I am proud to rise in support of H.R. 6304. I would like to thank Chairman REYES, Chairman CONYERS, Majority Leader HOYER, Minority Leader BLUNT, and Ranking Member HOEKSTRA for coming together with a bill that we need on behalf of our country.

My district includes the National Security Agency, and many of NSA's employees are my constituents. As a

member of the House Committee on Intelligence and the chairman of the Subcommittee on Technical and Tactical Intelligence, which oversees NSA, I know that the men and women who work for our Nation's intelligence agencies work hard every day to keep our Nation safe.

The intelligence agencies must do their work within the laws of this country, and they need those laws to be clear. The NSA employees in my district need a clear law with a bright line between legal and illegal surveillance activities, and this bill provides that.

Our Constitution requires checks and balances for the three branches of government. This bill provides that the FISA Court must review surveillance requests to protect the constitutional rights of our citizens.

I urge my colleagues to support this bill because it gives our intelligence community the tools they need to keep our Nation safe while protecting the constitutional rights of Americans.

Mr. HOEKSTRA. I would like to yield 3 minutes to another distinguished gentleman from Michigan (Mr. ROGERS).

Mr. ROGERS of Michigan. Madam Speaker, I want to compliment Mr. REYES. When this happened 124 days ago when it expired, I realized what a challenge you had. They were asking you to win the Kentucky Derby by entering a donkey in the race. And trying to get all of the folks together to get us to the place where we are today was not short feat.

Mr. Hoekstra and Mr. Reyes, I want to thank you both because what this bill does today is reaffirm what we have been saying for the last several years, that the due process of the Constitution, the fourth amendment, is alive and well and protected in this bill. And any rhetoric to the contrary is simply not true. It is fear mongering.

For any U.S. citizen who believes that their phones are going to be unceremoniously and injudiciously tapped or listened to is simply wrong, and this bill reaffirms the importance of that fourth amendment and due process for every American citizen every day.

But it also says some very important things. We are going to protect the Good Samaritan law that we have known and developed over the last 200-plus years that if you in good faith help your neighbor or help your country, in good faith you will be protected from damages sought by anyone else. If you stand up and protect the liberties and justice of your country and the lives of your neighbors, you will be protected in this law.

And finally, our foreign intelligence service allies have been nervous for 124 days, begging, pleading, cajoling, asking please, step up to the plate and reengage in one of the most important intelligence elements that we have, that the United States shares with our foreign allies to stop suicide bombers,

to stop terrorist elements from developing plans and plots to kill their citizens as well as our own.

This bill reaffirms all that we said last year and the year before. It reaffirms what we said in the Protect America Act in August of 2007 that it is absolutely important that we step up to the plate and listen to foreign terrorists in foreign lands plotting to kill citizens of our allies and here at home.

I want to congratulate all those who came together today, and urge those with the rhetoric to please stand for your country today, stand for the soldiers in the field who deserve our protection and the protection of the intelligence services, and for every mother and every father, every child in America who looks for a better day tomorrow knowing that we once again have both our eyes and our ears on the problem with terrorism and radical jihadists.

Mr. CONYERS. Madam Speaker, I am pleased to yield to the gentleman from New Jersey (Mr. Holt), a distinguished member of the Intelligence Committee, 1 minute.

Mr. HOLT. Madam Speaker, I thank the chairman of the Judiciary Committee for yielding me time to speak about this.

Unfortunately, the negotiators who brought this bill to the floor bought into the flawed assumptions of the Bush administration that because we live in a dangerous world, we must now redefine the fourth amendment and thus the fundamental relationship between the government and its people.

If this bill becomes law, it will perhaps be the only lasting legacy of the Bush-Cheney administration's overhaul of national security policy, a congressionally blessed distortion of congressional checks and balances. It permits massive warrantless surveillance in the absence of any standard for defining how communications of innocent Americans will be protected; a fishing expedition approach to intelligence collection that we know will not make Americans more safe.

Its court review provisions are weak and narrowly defined. I know some of those who negotiated this bill say that some court review is better than no court review. That is only true if the judge's hands aren't tied in the review process. They are in this bill.

There is a fundamental American principle that those who search, seize, intercept and detain should not be the ones who decide who are the bad guys.

Mr. SMITH of Texas. Madam Speaker, I yield 2 minutes to the gentleman from California (Mr. ISSA) who is a member of the Judiciary Committee and the Permanent Select Committee on Intelligence as well.

(Mr. ISSA asked and was given permission to revise and extend his remarks.)

Mr. ISSA. Madam Speaker, I rise in strong support of this hammered-out compromise bill.

You know, Madam Speaker, elections matter. The current balance in the

House and the Senate played an important part in the administration, House Republicans, House Democrats, Senate Democrats, and Senate Republicans coming together and figuring out what was needed, what was constitutional, in a very much bipartisan fashion.

Unfortunately, there are those who want to have it both ways, those who will talk about how this is balanced, it meets the needs of the administration, as the administration is assuring us, and it meets all of the constitutional requirements. But there are those who want to also play to the other side. While making sure that we are protected by a good piece of legislation, there are those who will come on the floor and denounce this and then vote against it.

Madam Speaker, I ask the American people to look long and hard at how people vote on this. This is in fact worked out to assure the American people, and properly so, that we will protect all of their constitutional rights while doing everything we can to ensure their safety.

This is good legislation worked out over a long period of time, and a lot of thoughtful work went into it on both sides. But I ask the American people to hold accountable those who would want to know that the American people are protected, and then vote against it in order to play to special interests.

Madam Speaker, that is the bad part of what will happen today. The good part is that America will be safer and the Constitution will be secure because of what we are doing here today. I thank you and urge support.

Mr. CONYERS. Madam Speaker, I am pleased now to yield to the gentle-woman from California (Ms. Lee), cochair of the Progressive Caucus and a leader in the Congressional Black Caucus, 1 minute.

Ms. LEE. Madam Speaker, let me thank the gentleman for yielding and for his leadership.

I rise in strong opposition to this very terrible bill. It does not strike the proper balance between protecting national security and preserving our cherished civil liberties.

Now I know how important those protections are from my personal experience with unwarranted domestic surveillance and wiretapping during the J. Edgar Hoover period. The government's infamous COINTELPRO program ruined the lives of many innocent persons. Others, including myself, had their privacy invaded even though they posed absolutely no threat to national security. We all remember how Dr. King and his family were the victims of the most shameful government-sponsored wiretapping. We must never go down this road again. Yet here we are again.

This bill undermines the ability of Federal courts to review the legality of domestic surveillance programs, it provides de facto retroactive immunity to telecom companies and does not sunset until December 31, 2012. How can we do that? Four years is way too long.

A good bill will protect Americans against terrorism and not erode the fourth amendment. This bill scares me to death, and I urge a "no" vote.

Mr. SMITH of Texas. Madam Speaker, I yield 3 minutes to the gentleman from California (Mr. DANIEL E. LUNGREN), a senior member of the Judiciary Committee and the Homeland Security Committee.

Mr. DANIEL E. LUNGREN of California. Madam Speaker, I thank the gentleman for the time.

Madam Speaker, as some say on radio, "Now let's hear the rest of the story." After the arguments just made on this floor, this is actually a great day. We and the American people have been waiting for this since 12:01 a.m. on February 6 when the Protect America Act expired. During the intervening time we have actually been unnecessarily vulnerable to those who would do us harm in this era of worldwide terrorism.

In fact, Madam Speaker, I would say that this is the single most important bill we will vote on this year, not that I say supporting our troops is not important, but the intelligence that we gather as the result of the authority granted by this bill may actually create conditions under which we do not have to send troops anywhere in the world and may be more protective of our rights than any other single thing.

Having come before this body on five different occasions since that initial expiration of the Protect America Act, I am greatly relieved that we can finally send the intelligence community and the American people a bill which will enable the intelligence community to continue to protect those American people.

Although the compromise agreement embodied in the proposal before us is not necessarily the one I would have written, it does, in my estimation, meet our responsibilities for protecting the American people. In other words, Madam Speaker, it is not the Mona Lisa but it is not a bad paint job.

First and foremost, the proposal before us ensures that we will continue to have the ability to monitor the conversations of al Qaeda overseas. And although there are requirements that the Attorney General and the Director of National Intelligence adopt procedures which will be submitted to the FISA Court, the bill retains sufficient flexibility for our overseas intelligence mission.

In other words, the intelligence community leadership has assured us that this bill will allow them the operational authority to do what needs to be done within the parameters of the Constitution. Both the safety of the American people as well as their civil liberties are protected in this proposal.

This proposal embodies compromise language which responds to the legitimate concerns of telecommunication providers who themselves responded to the call of their government in the wake of 9/11. The language of the bill not only satisfies the interest of justice, but communicates loudly to all Americans that if they are ever confronted with such requests, lawful requests, their government will not hang them out to dry afterwards.

Specifically, a Good Samaritan safe harbor will exist with respect to any civil action where there is substantial evidence to support the certification provided by the Attorney General. The quantum of evidence required is merely a showing of more than a scintilla but less than a preponderance of evidence.

And although these provisions in the proposal will contribute to securing the safety of our citizens, this is not to suggest that I support every provision in the compromise.

The SPEAKER pro tempore. The gentleman's time has expired.

Mr. SMITH of Texas. I yield the gentleman 1 additional minute.

Mr. DANIEL E. LUNGREN of California. For example, the so-called "exclusive means" language in the bill is seen by some as an assertion of maximal congressional authority. Let me just remind my colleagues that the FISA Court of review has said all of the other courts to have decided the issue held the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. The court stated that "we take for granted that the President does have that authority."

So regardless of whether we have a President McCain or a President Obama, this language will likely be interpreted in the context of facts in individual cases in light of the constitutional jurisprudence which has arisen with regard to the collection of foreign intelligence.

In other words, it does not either trample upon the constitutional prerogatives of the Congress nor those constitutional prerogatives of the President of the United States. This is a good compromise. It protects the American people. We have been waiting for it. It ought to be voted on with dispatch.

Mr. REYES. Madam Speaker, I yield 2 minutes to the distinguished gentleman from Rhode Island (Mr. Langevin), a valued member of our Intelligence Committee.

(Mr. LANGEVIN asked and was given permission to revise and extend his remarks.)

□ 1145

Mr. LANGEVIN. Madam Speaker, I rise in support of the FISA Amendments Act of 2008. Though not a perfect piece of legislation, it is clearly far better than what we have today, and addresses a number of the many concerns that were raised about the administration's conduct of surveillance in this country.

As a member of the Intelligence Committee, I know that we must give our Intelligence Community the proper tools to protect us, while upholding the civil liberties of Americans. Today's compromise illustrates what this House can do when it deliberates with care, holds steady against fear mongering and acts in the best interests of the country and its citizens.

This bill is strong on civil liberties, and includes protections against infringement of our constitutional right to privacy.

First, the bill clarifies that FISA is the exclusive means by which the executive branch may conduct electronic surveillance on U.S. soil. No President will have the power to do an end-run around the legal requirements of FISA. This provision will prevent the types of abuses we've witnessed under this administration.

Second, this act requires a warrant from the FISA court to conduct surveillance of Americans abroad. Americans will no longer leave their constitutional protections at home when working, studying or traveling abroad.

Third, it requires prior approval by the FISA court of procedures the government will use when carrying out foreign electronic surveillance. This will ensure that the government's efforts are not aimed at targeting Americans, the so-called reverse targeting that we're all concerned about; and that if an American's communications is inadvertently intercepted, it is dealt with in a manner that guarantees legal protections.

It also requires and allows for, now, an IG investigation of this warrantless surveillance program that took place prior to Congress being made aware of this legislation.

The SPEAKER pro tempore. The gentleman's time has expired.

Mr. REYES. I grant the gentleman another 15 seconds.

Mr. LANGEVIN. Madam Speaker, as I've said before, this legislation will only work if everyone involved follows the rules and remains within the confines of the law. Congress must continue to conduct robust oversight to make sure that the law is implemented as intended to maintain the critical and fragile balance of protecting our Nation and protecting civil liberties.

Mr. HOEKSTRA. At this time I would like to yield 1 minute to the gentleman from California (Mr. ISSA).

(Mr. ISSA asked and was given permission to revise and extend his remarks.)

Mr. ISSA. Madam Speaker, in just 1 minute it's impossible to assure the American people of everything this bill will do. But I would like too, if you will, react to something that was said on the other side that just simply isn't true

Yes, during J. Edgar Hoover's day, there was warrantless surveillance, even on political enemies of the people who were President at the time. Those days are behind us.

This act, long since we've taken care of domestic wiretap, but this goes one step further. It insures Americans and particularly, I think, Arab Americans like myself who might go back and forth between here or have relatives in the Middle East, that their conversations will not be the subject of warrantless wiretaps, that, in fact, they can be very confident that America is going to observe the Constitution for them, both when they are here and if they are visiting abroad.

So it's not easy to undo some of the statements that talk about the past, but the truth is, this will protect what has already been established for Ameri-

cans here.

Mr. CONYERS. Madam Speaker, I am pleased to yield to the gentleman that has more measures in the Judiciary Committee than anybody else in Congress, Dennis Kucinich, the distinguished gentleman from Ohio, 1 minute.

Mr. KUCINICH. Under this bill, large corporations and big government can work together to violate the United States Constitution, use massive databases to spy, to wiretap, to invade the privacy of the American people. There's no requirement for the government to seek a warrant for any intercepted communication that includes a U.S. citizen, as long as the program in general is directed towards foreign targets.

This Congress must not allow the names of innocent U.S. citizens to be placed on secret intelligence lists. Under this bill, violations of Fourth Amendment rights and blanket wiretaps will be permissible for the next 4 years. Massive and untargeted collection of communications will continue and with the enactment of this bill.

Furthermore, it allows the type of surveillance to be applied to all communications entering and exiting the United States. These blanket wiretaps make it impossible to know whose calls are being intercepted by the National Security Agency.

Let's stand up for the fourth amendment. Let's remember, when this country was founded Benjamin Franklin said, those who would give up their essential liberties to achieve a measure of security deserve neither. Vote against it.

Mr. SMITH of Texas. Madam Speaker, I yield myself the balance of my time.

Madam Speaker, H.R. 6304 may well be one of the most important pieces of legislation we pass this Congress.

For 4 months America has been more vulnerable to attacks by our enemies, because of the refusal by some to bring a commonsense bill to the floor to help the Intelligence Community protect Americans.

Many of us would have preferred the bill passed by the Senate. Although this bill may not be ideal, it does represent a compromise between House and Senate Republicans and Democrats. This compromise preserves our ability to conduct a strong, effective foreign intelligence program.

I urge my colleagues to support this legislation.

Madam Speaker, I yield back the balance of my time.

Mr. REYES. Madam Speaker, it is now my pleasure to yield 1 minute to our esteemed Speaker of the House, Ms. PELOSI.

Ms. PELOSI. Madam Speaker, I thank the gentleman for yielding. I thank him for his great leadership as the chairman of the Intelligence Committee. I commend him.

I commend Mr. Conyers, the distinguished chairman of the Judiciary Committee, for although he is not supporting the legislation before us today, he certainly had a tremendous impact to improve it. Thank you for your relentless championing of civil liberties in our country, Mr. Conyers.

I want to pay special tribute to our majority leader, Mr. HOYER, for making this compromise possible today. It's a very difficult task, many competing views as to how we should go forward. Mr. HOYER handled it all with great intellect and great respect for all of those views. Thank you, Mr. HOYER.

Also want to acknowledge Mr. SMITH and Mr. HOEKSTRA and minority whip, Mr. BLUNT, for their leadership in giving us this opportunity today.

We've heard it over and over again. Our colleagues say this bill is not perfect, this isn't the bill I would write. I prefer this bill, I prefer that bill.

Well, I prefer the House bill that passed and was sent to the Senate. It isn't an option for us. I do not, I totally reject the Senate bill which is an option, and that is the comparison that we have to make, the contrast that we have to make today.

But in doing so, I think we all understand the important responsibility that we have in this Congress, focused on this debate today. I always take the debate back to our responsibility when we take the oath of office. We take an oath of office to protect and defend the Constitution from all enemies, foreign and domestic. In that preamble to our Constitution, we must provide for the common defense. Essential to honoring that commitment to protect the American people is to have the intelligence, operational intelligence that will help us do that.

When I first went on the Intelligence Committee, our focus was on force protection. Our troops in the field depend on timely and reliable intelligence to make the decisions necessary to keep them safe and to do their job. Force protection, force protection, force protection. It is still a primary responsibility of our intelligence.

In addition to that, we have the fight on the war against terrorism, the fight against terrorism, wherever it may exist. Good intelligence is necessary for us to know the plans of the terrorists and to defeat those plans.

So we can't go without a bill. That's just simply not an option. But to have a bill, we must have a bill that does not violate the Constitution of the United States, and this bill does not.

Some in the press have said that under this legislation, this bill would allow warrantless surveillance of Americans. That is not true. This bill does not allow warrantless surveillance of Americans. I just think we have to stipulate to some set of facts.

We may have our opinions about the bill, but there have been so many versions of the story of different bills that have come up, the PAA last year, which I thought was totally unacceptable. The Senate bill, also unacceptable. Our House bill, which I mentioned before, which I thought was the appropriate way to go, and now this compromise.

As I was talking with Mr. HOYER in the course of his negotiations, there were certain things that I thought had to be in the bill to make it acceptable, certain threshold issues that had to be there, and they are.

In terms of the original FISA bill, it's interesting to note that this bill is an improvement on that in three important ways.

First, we all recognize the changes in technology necessitate a change in the legislation, and this legislation today modernizes our intelligence-gathering system by recognizing and responding to technological developments that have occurred since the original FISA Act in 1978. In doing so, we can make the country safer in a more advanced technological way.

Second, and this is very, very important, and there's some misunderstanding about this. This bill provides that Americans overseas receive the same FISA protection, including an individualized warrant based on probable cause, as Americans living within the country. This is a very important improvement on the original FISA Act.

Third, this bill strengthens congressional oversight. And this is very important, the transparency. Transparency and intelligence don't always go together, but accountability is central to intelligence. This strengthens congressional oversight by requiring that the executive branch provide more extensive information about the conduct of surveillance to both the Intelligence Committee and the Judiciary Committee. This is new, this is better. The more we know, the better, I think, the law will be enforced.

If this bill does not pass, we will most certainly be left with the Senate bill. I think that's clear. And this bill is an improvement over the Senate bill in the following ways, just to name a few.

First of all, it reaffirms that FISA is the exclusive means of collecting foreign intelligence, and makes absolutely clear that the enactment of an authorization for the use of force does not give the President, whoever he may be, any inherent authority to alter the requirements of FISA. Very important.

This is important because President Bush believed, and this was what we were told, that he, as President of the United States, had inherent authority under the Constitution to do almost anything he wanted.

And what this bill reaffirms is that the FISA law is the authority for collecting foreign intelligence. There is no inherent authority of the President to do whatever he wants. This is a democracy. It is not a monarchy.

Secondly, it is an improvement of the Senate bill. And by the way, no offense to President Bush. I wouldn't want any President, Democrat or Republican, a Democratic President or a Republican President to have that authority.

Secondly, the bill provides that, except in rare circumstances there will be pre-surveillance review by the FISA Court.

\square 1200

And when I say rare circumstance, I mean very, very rare.

Unlike the Senate bill, this legislation retains FISA's broad definition of electronic surveillance and thus guarantees that basic protections of FISA apply to all the new forms of collection authorized by the bill. There had been an attempt, and that's why the Senate bill is inferior in this respect, to just narrow it to certain kinds of collection, and this says it applies to all collection, electronic surveillance.

Fourth, it contains specific protections against reverse targeting. This reverse targeting is very, very important to the civil liberties of the American people, and I am satisfied by the specific provisions against reverse targeting. It provides a full and independent review of the President's surveillance program by the Inspector General of the relevant agencies.

Of course, there are aspects of this compromise bill that I do not like. I don't believe that Congress should be in the business of interfering with ongoing lawsuits and attempting to grant immunity to telecommunication companies that allegedly violated the law. Those companies have not lived up to a standard expected by the American people. I don't think today is any cause for celebration for them. They come out of this with a taint.

I do not believe that the pending lawsuits would have achieved what we would have liked them to do which is what the Inspector General's review would, which is to learn the truth about the President's terrorist surveillance program and give us the information we need to make sure that never happens again.

In addition, this legislation makes sure that in the future, the telephone companies must fully comply with Federal statutes.

Again, it would have been my preference to vote for the RESTORE Act that the House sent over to the Senate. I do not consider it an option to live with the Senate bill. This is the opportunity that we have to protect the American people through the gathering of intelligence which is essential, as I said earlier, to force protection, to protect our men and women in uniform and help them make the decisions they need to do their jobs and keep them

safe and to fight terrorists by learning their plans in advance and squelching them

I want to thank those who have worked so hard to bring this bill to the floor. Again, it's not a happy occasion, but it's the work that we have to do. I think we have to remember getting back to the Constitution. The House, article 1, legislates. We pass the laws. The judiciary interprets the law. The executive branch enforces the law. And what is very important about whatever we pass, especially in relating to subiects relating to our security and our liberty, it's important that the President of the United States enforce this law honoring the Constitution of the United States recognizing the responsibility that we all have to protect the American people and protect the Constitution of the United States at the same time.

So again, a difficult decision for all of us. I respect every opinion that was expressed on this floor today. The knowledge, the sincerity, the passion and the intellect of those who support and oppose this have been very, very valuable in making the bill better, if not good enough for some, but certainly preferable to the alternative that we have which is the Senate bill which must be rejected.

I'm not asking anybody to vote for this bill. I just wanted you to know why I was

Thank you, Madam Speaker.

Mr. HOEKSTRA. Madam Speaker, I would like to yield myself the balance of my time.

In the immediate aftermath of 9/11, the President, the leaders of Congress, faced a very difficult situation: to learn more and to better understand the threat that America now faced. They recognized that we needed to move from a mentality of being law enforcement to a mentality of prevention, that we needed to confront, contain, and ultimately defeat radical jihadists if America was going to stay safe.

The President, the leaders of Congress, many of whom spoke today, huddled together and talked about the various strategies that they could implement to get a better understanding of this organization called al Qaeda, its leaders, its intentions, and its capabilities.

Overarching in their discussions were making sure that the Constitution and the rule of law would guide their behaviors. As they considered various alternatives and discussed these, they implemented a terrorist surveillance program using the capabilities that in many cases are unique to America that could give us insights into al Qaeda, its leadership, and its intentions.

It's not the President's program. This program was put together by the President in consultation, sure, with members of his cabinet, but also, very importantly, with consultation on a bipartisan basis with the leaders of Congress

These leaders in Congress were consistently briefed about how the program would work, the kinds of information that was being obtained, and how it was being used to keep America safe, all the while placing a responsibility on yes, the President, but also the leaders of Congress to make sure that the intel community was doing the things it was being asked and was being asked to do things that would be legal.

The intel community has performed very well. They have gotten us information that has enabled us to keep America safe. The intel community, this administration, and Congress asked other parts of our economy to participate, private sector companies. They stood up and they did the job to keep America safe. Congress did the necessary job of doing oversight, and in 2004, we reformed the intelligence community

So since 9/11, many things have been done properly. The end result, as we've gone through this process, is that we have kept America safe.

I congratulate the Speaker, I congratulate the majority leader, I congratulate my colleagues on the other side of the aisle, Mr. SMITH, for working in a bipartisan basis to recognize what needed to be done in allowing this bill to come to the floor and continue to move forward in a slightly different way than how we've been moving forward over the last 6 years. But the most important thing is in a bipartisan basis, we have come together on a national security issue to give our intelligence community the tools that they need to keep America safe.

Mr. CONYERS. Madam Speaker, I would like now to recognize the distinguished gentleman from Washington, JAY INSLEE, for 1 minute.

Mr. INSLEE. Have we forgotten what our ancestors have done in the cause of liberty? Don't we realize there are some lines we can never cross? Don't we realize we should never legitimize illegal violations of America's privacy rights, which this bill does?

This bill says if the telecommunication companies violated America's privacy willfully, knowingly, knowing it was illegal, we are giving them immunity. Where is the excuse for that? Where is the excuse for turning a Nation of laws into a Nation that will be led by a President who knows how to manipulate our fears?

We have got to know the law is our ultimate guardian of liberty, and those on this side have accused us of having a pre-9/11 mentality. Let me remind them that July 4, 1776, was pre-9/11. And heaven help us the day that those values are shucked aside at the service of fear.

Reject this bill.

Mr. CONYERS. Madam Speaker, I will take this time to use the remaining time that is allotted me.

The SPEAKER pro tempore. The gentleman is recognized for 1 minute.

Mr. CONYERS. I would like to point out that the grant of retroactive immunity to the telecoms is inconsistent with our basic principles because we are breaking with a very proud tradition of intervening for the first time in a pending court decision in an effort to reach a preordained legal outcome. This is a bad precedent.

And may I point out, too, that we are in a period in which the executive branch has been deemed by many constitutional authorities to be very near the description of an imperial Presidency. We've gone too far.

I hope that we will get a strong vote against this because the struggle for restoring our precious rights and liberties must continue.

I return all time that may be remaining on our side.

Mr. REYES. Madam Speaker, how much time remains?

The SPEAKER pro tempore. The gentleman from Texas has $2\frac{1}{4}$ minutes.

Mr. REYES. Madam Speaker, it is my privilege to yield 1 minute to our distinguished majority leader, Mr. HOYER, who in this case deserves MVP status for having the wisdom of Solomon and the patience of Job.

Mr. HOYER. I thank my friend, the chairman of the Intelligence Committee. I thank the Speaker. I thank the Speaker not only for giving me the responsibility for trying to work with some extraordinarily talented people but also for having the courage to lead and the courage to express her convictions.

And I want, at the outset, to share her view that every Member who has spoken on this floor has spoken out of a sense of conviction and out of a sense of responsibility to the Constitution of the United States and to the protection of our great Nation and our great people.

Mr. REYES, Mr. CONYERS, Mr. HOEK-STRA, Mr. SMITH have all worked to come together, realizing that there were significant differences. Those four have been assisted by some extraordinary people, and at the outset, I want to mention them.

First of all, I want to mention my own staff without whom I think we would not be at this day. She sits on the floor. She worked for my colleague and dear friend Senator Paul Sarbanes for a number of years. One of the benefits of Senator Sarbanes retiring was that she came to my staff. Mariah Sixkiller has expended too much time, perhaps, but with great talent and great ability to reach this day. Thank you, Mariah Sixkiller.

I want to thank Chairman Conyers because Chairman Conyers, as you've heard on the floor, has been conflicted but he has been focused on the necessity to respond to issues that are real and also to help us move forward so that we did not, in the minds of many of us, have a bill pass that we thought was unacceptable, a bill passed by the Senate with 68 of 100 votes. We would not be here, in my opinion, without Chairman Conyers' leadership, not because he supports this alternative, but because he saw the ability to work together.

I want to thank his staff, Lou DeBaca, Perry Apelbaum. And Lou DeBaca, in particular, who sat for hours and hours and hours in a room trying to reach agreement as we made compromises. Mr. REYES' staff, Mike Delaney, the staff director. Jeremy Bash. Jeremy Bash did extraordinary work. Jeremy Bash was hired by the former Chair of the Intelligence Committee, Jane Harman.

Jane Harman is probably as knowledgeable as almost anybody on this floor, other than perhaps the Speaker who served on the Intelligence Committee longer than anybody in this House. Jane Harman's leadership, concern, focus on constitutional rights, focus on the security of our country, was outstanding. She played a significant role in trying to get us to this day.

□ 1215

Eric Greenwald of Mr. REYES' staff also played a significant role.

Without Mike Sheehy and Joe Onek of the Speaker's staff, we would not be here today. We would not have reached the good compromises that we reached. Joe Onek and Mike Sheehy, if they were writing this bill, would have written a different bill, much closer to what we passed on our side of the aisle and sent to the Senate, which they rejected. Mike Sheehy has served the House and the Speaker for a very long time in the intelligence field.

I want to thank Senator ROCKE-FELLER. We would not be here today on this floor if it were not for Senator ROCKEFELLER. Senator ROCKEFELLER very early on had discussions with me about what could they do to try to move towards the bill that we passed. He made some suggestions. Those suggestions are in this bill today. He facilitated our actions. Andy Johnson, Mike Davidson, Alissa Starzak of his staff were very, very helpful.

Senator Bond, Senator Bond and I did not see necessarily eye-to-eye on these issues as we began, but at the end, we came to an agreement. Louis Tucker and Jack Livinston of his staff were very helpful.

Chairman HOEKSTRA, or former Chairman HOEKSTRA, now Ranking Member HOEKSTRA, I want to thank Chairman HOEKSTRA, but particularly, I want to thank Chris Donessa who was very helpful, gave us great assistance and advice.

LAMAR SMITH and Caroline Lynch of his staff, thank you very much for your efforts as you sat in that room, as we all sat around, every one of the committees sat around the table, as we came to the final agreement.

Then I want to thank, of course, Jen Stewart and the minority leader, without whom we could not have gotten to this day.

Lastly, I want to thank my friend. There's an article going to be written. It's going to speculate whether or not he and I hurt one another by saying the other is his friend. I don't think that's

the case. I said that ROY BLUNT and I often disagree on substantive issues, but what we agree on very strongly is that this House needs to sit down and talk to one another and try to reach resolution on difficult issues, not hard-to-reach compromise on easy issues. It's on the difficult issues.

ROY BLUNT is a man of this House, who cares about this House, who cares about this country. And he cares about drafting legislation that can be agreed upon by a broad section of this House and the American people. He has an extraordinary staff of Brian Diffell, who I want to thank for his efforts, but in particular, I want to thank ROY BLUNT for his friendship, for his integrity, and for his willingness to take risks to reach compromise. Thank you, ROY.

Madam Speaker, today we conclude one step in a long, continuing process. Just under a year ago, the House came under great pressure from the administration and the Senate to pass the Protect America Act, a bill I could not support and spoke out against for its lack of civil liberties protections.

Since then, there have been other attempts to modernize the Foreign Intelligence Surveillance Act: first, the RE-STORE Act passed by the House last November with my strong support, with Mr. Conyers' strong support, Mr. REYES' strong support, and the support of this House; that was followed by the Senate bill which passed, as I said earlier, with 68 votes in February; and most recently, the FISA Amendments Act, passed by the House last March. I supported that bill as well. I think it was a better bill. It would be my alternative. It was our alternative on this side of the aisle, but it was not the consensus alternative, and we needed to reach consensus to move forward.

I was proud to support the two House bills, which I believe struck the right balance between giving our intelligence community the tools to go after those who seek to harm and protecting the constitutional rights of American citizens.

Today, I stand in support of a different kind of bill, a compromise. To be clear, this is not the bill that I would have written or that perhaps anybody individually on this floor would have written. However, in our legislative process, no one gets everything he or she wants. Different parties, often with deeply competing interests, come together here to produce a consensus product, where each side gives and takes. I don't believe we've given on the ultimate principles on either side.

Over the past few months, I've been involved in almost daily discussions with the stakeholders on this important issue, Members in both Chambers, in both parties, as well as outside organizations and experts. I want to thank all of the outside organizations, whether they agree with our product or do not. Their contribution has been an important one. I particularly want to thank those who take very unpopular

positions to protect the rights of perhaps just one of us among the 300 million, who in the land of the free and the home of the brave deserve to have that one individual right protected, and I appreciate their efforts to ensure that that country remains that kind of country.

Together, we have worked to develop a bill that strikes a sound balance. This measure provides the intelligence community with the strong authority to surveil foreign terrorists who seek to harm this country and our people. As the Speaker said, that is our responsibility, and we intend to meet it.

It provides for enhanced civil liberties protections for Americans and insists on meaningful judicial scrutiny.

It includes critical new oversight and accountability requirements that both address the President's warrantless surveillance program and ensures that any surveillance going forward comports with the fourth amendment and will be closely monitored by the Congress.

Of vital importance, my colleagues, this legislation makes clear that FISA is the exclusive means by which the government may conduct surveillance, the Foreign Intelligence Surveillance Act. Contrary to the administration's previous actions, in which it did not comply with the FISA statute, this statute makes it very clear, this and this alone is the process through which we will intercept communications, an issue of great importance to the Speaker, as she has said.

Notably, this bill does not address or excuse any actions by the government or government officials related to the President's warrantless surveillance program, nor does it include any statement by the Congress or conclusion on the legality of that program.

Indeed, it mandates for the first time ever a robust accounting by the Inspectors General of the warrantless surveillance program, which Congress will receive and act on.

Madam Speaker, in closing, let me say again, this bill is a compromise, but in my opinion, it is a compromise worth supporting. And the conclusions drawn by editorials in the New York Times, Wall Street Journal and Washington Post over the last 2 days reflect this compromise.

Today, for example, the Washington Post recognized that this is a reasonable effort to strike a compromise, stating: "Striking the balance between liberties and security is never easy, and the new FISA bill is not perfect. But it is a vast improvement over the original law and over the earlier, rushed attempts to revise that law."

As I said at the beginning, this bill is one step in a long, continuing process of updating this critical legislation, ensuring that our national security and our civil liberties are both protected.

This legislation sunsets at the end of 2012, and it's imperative that we scrutinize its implementation in the future and make any necessary changes. I be-

lieve we have the best bill before us that we could possibly get in the current environment. It is a significant improvement over the Senate-passed bill and, I suggest, existing law.

I look forward to working with my colleagues in the years ahead to ensure that both our national security and our civil liberties are protected. That is our responsibility. That is our pledge to our constituents. I urge passage of this legislation.

Mr. REYES. Madam Speaker, I yield myself the balance of the time.

I just wanted to thank everyone again, as Mr. HOYER indicated. I believe every Member in this body cares about our national security, and I also believe that this is a good bill, a good compromise and is worthy of supporting.

Mr. VAN HOLLEN. Madam Speaker, on March 14th I voted in favor of H.R. 3773 which modernized the Foreign Intelligence Surveillance Act. This bill successfully updated the law to accommodate the current day communications technology while at the same time providing the much-needed protection of the court in sanctioning the surveillance of Americans. Moreover, the bill was also remarkable for what it did not contain; it did not provide retroactive immunity for telephone companies who are defendants in pending lawsuits. These suits have been brought to uncover the full extent of the Administration's program to conduct unauthorized surveillance on Americans.

I am deeply troubled that the Senate does not have the votes to pass the House bill. The Senate instead passed its own bill, S. 2248, which was unacceptable to me from the outset because it reduced the role of the FISA Court to merely review the procedures for targeting surveillance subjects and minimizing the information collected. Moreover, the Senate bill established retroactive immunity for the phone companies that have been used to carry out the Administration's illicit surveillance program.

To be sure, the Senate bill is completely unacceptable. Majority Leader HOYER worked tirelessly to improve upon the Senate bill to forge an acceptable compromise. The bill before us today, however, does not go far enough to include sufficient safeguards of court involvement in the surveillance of Americans. Moreover, it continues to provide retroactive immunity for those companies that carried out the Administration's unauthorized surveillance. Finally, it fails to hold the Administration accountable for its past illicit surveillance activities and its disregard of the Fourth Amendment protections of Americans. As a result, I must vote against this bill.

Ms. SPEIER. Madam Speaker, when are we going to stop pulling the wool over the eyes of the American people? The proposed FISA law protects no one other than the administration and those within it who may use this newfound power to snoop and spy in areas where they have no business looking. We are giving broad new powers to political appointees who have repeatedly disregarded the Constitution and ignored the most basic rights of Americans to live their lives without Big Brother peeking his nose into their private matters.

This FISA bill gives the federal government sweeping powers to gather wide swaths of information from foreign sources while providing little or no justification for the national security value of that information.

The FISA Court set up to police the process isn't a court at all. Under this bill, the government can gather as much intelligence as it chooses for seven days prior to going to the court. Then, if the court says "No" to the request, the government can continue to gather intelligence for 60 days while they appeal.

Any first year law student knows that is not how courts work. If this were a real court, the government would be required to abide by the decision of the court and seek the warrant prior to conducting surveillance.

It is fundamentally untrue to say that Americans will not be placed under surveillance after this bill becomes law. The truth is, any American will subject their phone and e-mail conversations to the broad government surveillance web simply by calling a son or daughter studying abroad, sending an e-mail to a foreign relative, even calling an American company whose customer service center is located overseas

Once again, our government puts a feel-good name on something that doesn't live up to its billing. Calling the FISA rubber stamp panel a court is akin to the President's "Clear Skies Initiative" which relaxed pollution regulations or "No Child Left Behind" which instead of helping schools, punishes them if they have children who are, indeed, lagging behind.

This bill sets out to reassure Americans that, because there are warrants and a "court", due process is taking place. But like the pseudo-court, FISA warrants aren't warrants at all.

A warrant is permission by the court to look for a specific thing from a specific person or group for a specific reason. The FISA warrant is given after the fact and can be as broad as gathering all electronic communication coming into or out of a foreign country.

Madam Speaker, America isn't simply 'guided" by our Constitution, it isn't a set of "suggestions" but rather, the law of the land. It is the existence of this great document and our unswerving loyalty to it that makes America the greatest nation in the history of our planet. We can't be sacrificing basic constitutional principles like the fourth amendment simply because it's an election year and we want to make it look like we're fighting terrorism.

I join my colleagues in our unified fight to defeat the global terrorist movement. But we don't do that by sacrificing our hard-earned Constitutional rights and forgiving telephone companies who knowingly violate those rights.

The bottom line is, this FISA bill permits the collection of Americans' emails and phone calls if they are communicating with someone outside of the U.S. This is especially true when it comes to emails, because the World Wide Web has no area codes, so it is impossible to tell where email communications originate from. The Government is under no obligation to seek a warrant in order to monitor an email account unless it knows the account belongs to an American.

And once your email account is swept up in the system, it can be monitored. Regardless of the relevance of your personal information, once it is gathered by the government, it is never destroyed. One only has to recall the recent incident in the State Department where candidates' passport information was breached to know that this information isn't

handled by robots, but people. And people can do any number of things with personal informations.

Out of respect to the United States Constitution and the basic rights of Americans to live free of intrusive eavesdropping by their government, I strongly oppose HR 6034, the FISA Reauthorization Act.

Ms. ESHOO. Madam Speaker; first I want to commend the Chairman and the Majority leader for the work they've done to bring this legislation to the floor of the House. It has been a challenge for all of us on the Intelligence Committee and in the Congress.

This legislation is a vast improvement over the previous law, and indeed over the Protect America Act passed by the House last August which I opposed.

The bill very importantly establishes a process for electronic surveillance that includes prior approval by the independent courts, and in some respects, this legislation goes even further than the existing FISA statute or the House-passed RESTORE Act in protecting the civil liberties of U.S. persons. Under this bill the Administration would have to seek a court order before conducting surveillance on U.S. persons abroad. Until now and under the Protect America Act, the executive branch could conduct electronic surveillance of U.S. persons without prior judicial approval. This legislation also allows the lawsuits against the telecommunications companies to go forward in a limited fashion, which would not have occurred at all under current law.

Having said this I must oppose this bill.

Under the original structure of FISA, tele-communications carriers served an important gate-keeping function. They were not permitted to provide access to private communications in the United States unless the government made a lawful request to conduct surveillance, pursuant to a FISA order. For decades, the government has sought and obtained thousands of FISA warrants prior to beginning surveillance, or in urgent cases shortly thereafter. We all remember the shocking news when the President had to acknowledge that his Administration created an illegal, warrantless electronic surveillance program outside of the FISA legal framework.

This legislation would essentially grant retroactive immunity to telecommunications carriers who relied on statements made by this Administration that the program was lawful. However, as we've seen in numerous instances, this Administration pushed new and aggressive interpretations of the law, including in this area. We all recall vividly the days following 9/11, and the urgency that prevailed, but suspending our laws and allowing the Attorney General to unilaterally issue a "get out of jail free card" is not appropriate under any circumstances. There should be at least some minimal inquiry into whether the telecommunications carriers reliance on the statements made by this Administration was reasonable. If so, the they would be able to assert their existing statutory immunity defenses.

Throughout our Nation's history, the judiciary has been the most important check on an overzealous executive, and it is often through the judicial process that we uncover and remedy some of the most egregious executive misconduct. This legislation undermines and effectively nullifies the courts' ability to hold the Administration accountable for its actions, which likely violated the Constitution.

Our Nation was founded on the principle of separation of powers. The executive branch should be subject to independent oversight by the judicial branch. This legislation does not go far enough to allow the judicial branch to conduct an independent, reasoned inquiry into this critical issue. Therefore, I must oppose this legislation.

Mr. UDALL of Colorado. Madam Speaker, I will support this bill.

I will do so because, as I have consistently said, I do think the basic law in this area—the Foreign Intelligence Surveillance Act, or FISA—needs to be updated to respond to changes in technology, which was the purpose of the current, temporary law.

That is why, last August, I voted for a bill (H.R. 3356) to provide such an update—a bill that was supported by a majority of the House, but did not pass because it was considered under a procedure that required a two-thirds vote for passage, which did not occur because of the opposition of the Bush Administration. It was supported by all but three of our Republican colleagues.

That is also why I voted for another bill to update FISA—H.R. 3773, the "Responsible Electronic Surveillance That is Overseer, Reviewed, and Effective" (or RESTORE) Act—which the House passed on November 15th of last year. Like those bills I supported earlier, this bill will replace the Protect America Act, enacted in August 2007—which I opposed.

The bill makes it very clear that to conduct surveillance targeting a person in the United States, the government first must obtain an individual warrant from the FISA Court, based upon probable cause.

And, importantly, it explicitly states that FISA and Title III of the U.S. criminal code are the exclusive means by which the government may conduct surveillance on American soil, and adds that any future statute must expressly authorize surveillance if the government is going to rely on it to conduct domestic surveillance

It also includes new legal protections for Americans abroad, requiring an individual probable cause determination by the FISA Court when the government seeks to conduct surveillance of U.S. persons located outside the United States.

It requires prior review and approval by the FISA Court of the targeting and minimization procedures used to conduct surveillance of any foreign targets (unless in an emergency, in which case the government may authorize the surveillance and then apply to the FISA Court for approval within 7 days), and requires that this surveillance be conducted in accordance with the Fourth Amendment. And it requires the government to establish guidelines to ensure that Americans are not targeted by this surveillance ("reverse targeting guidelines"), and requires the government to provide those reverse targeting guidelines to Congress and the FISA Court.

The legislation also includes important provisions to increase transparency and accountability. For example, it requires there be a comprehensive review of the President's warrantless surveillance program by the Inspectors General of the Justice Department, the Directorate of National Intelligence, the National Security Agency, and the Defense Department—and it provides for them to report the results to the Intelligence and Judiciary Committees.

This report will review "all of the facts necessary to describe the establishment, implementation, product, and use of the Program," as well as "communications with, and participation of, individuals and entities in the private sector related to the Program."

I do not find equally satisfactory another aspect of the bill that involves accountability—the treatment of pending lawsuits against various telecommunication companies that acted to implement President Bush's clandestine surveillance program.

Like the bills I supported earlier, this measure would provide civil liability protection for private sector companies that provide lawful assistance to the government in the future. But it differs significantly in the way it addresses those pending lawsuits, which deal with the previous actions of the defendant companies.

Those lawsuits have been consolidated and are pending in one court, but evidently have made little progress because of the Administration's argument, still awaiting court resolution, that the suits are barred because they involve state secrets. My understanding is that the defendant companies have argued that government's invocation of the state-secrets privilege has had the result of preventing them from defending themselves, although at least one company has stated in regulatory filings that the cases against it are without merit.

President Bush has insisted that Congress throw these cases out of court by giving the companies retroactive immunity for whatever they might have done in connection with the surveillance program, even though the Administration and the companies themselves insist that those actions were lawful and that the plaintiffs' complaints against the companies have no merit.

Regrettably, the Senate decided to comply with the president's demand on this point, and its version of this legislation would provide that retroactive immunity. I do not think that was the right decision because I agree with the Rocky Mountain News, which in a February 15th editorial said "Letting this litigation proceed would not, as Bush [has] said . . .punish companies that want to 'help America.' Businesses that want to help America need to be mindful of the Constitution—and so should the government."

I supported removing that "state secret" barrier and allowing the companies to defend themselves by demonstrating to the court the evidence they say supports their arguments in a way that assures the continued security of that evidence and that avoids the public disclosure the Administration says would be adverse to the national interest. This is a process that has worked well in criminal cases, and while I am certainly not an expert on the matter, I think it can work when applied to these civil cases.

In that respect, this bill is similar to the legislation I supported earlier this year. But it is not identical, and I do not think it is quite as sound.

Under this bill, a district court hearing such a case will decide whether the Attorney General's certification attesting that the liability protection standard has been met and is supported by substantial evidence. In making that determination, the court will have the opportunity to examine the highly classified letters to the providers that indicated the President had authorized the activity and that it had been determined to be lawful.

That is not as strong a requirement for accountability as I would prefer. However, in such cases both plaintiffs and defendants will have the opportunity to file public briefs on legal issues and the court should include in any public order a description of the legal standards that govern the order.

And, importantly, this immunity provision does not apply to any actions against the Government for any alleged injuries caused by government officials.

Madam Speaker, as Benjamin Franklin has warned us, people who value security over liberty will get neither—and the Bush Administration has finally agreed to end its disregard for liberty and agree to effective judicial oversight and involvement in intelligence surveillance.

That agreement that is embodied in this bill, and the choice before us now is whether to reject it or to support the compromise measure now before us.

After careful review, I have concluded that the bill adequately meets the test of protecting civil liberties while giving our country tools needed to effectively combat terrorism.

So, while—like any compromise—the bill is not ideal, I have decided the correct decision—the one that will fulfill my responsibility to protect both our national security and the civil liberties that make our nation worth defending—is to vote for it.

Mr. ETHERIDGE. Madam Speaker, I rise in support of H.R. 6304, FISA Amendments Act. This bipartisan bill takes steps to increase our Nation's security while also protecting Americans' civil liberties.

H.R. 6304, FISA Amendments Act, provides the critical tools that our intelligence community needs to ensure the safety of our Nation. With many surveillance warrants set to expire in the coming weeks, the intelligence community needs a strong and dependable set of guidelines to follow while conducting surveillance. H.R. 6304 allows the Government to authorize surveillance in the case of an emergency situation, provided that they return to the FISA court within 7 days to apply for a warrant.

This bill also includes a number of provisions that significantly strengthen the protection of our civil rights. H.R. 6304 clarifies that FISA is the exclusive means for conducting surveillance in the United States, prohibiting any President from using executive power to conduct a warrantless wiretapping program. This bill also requires the Government to obtain an individual warrant from the FISA Court before conducting surveillance on a United States citizen. This warrant must be based on probable cause, and the provision now includes American citizens abroad as well. H.R. 6304 requires prior review and approval of the intelligence community's targeting and minimization procedures that ensure that any inadvertently intercepted communications by American citizens are destroyed. Finally, the FISA Amendments Act adds a strong layer of oversight to this process by directing the Inspectors General from Justice, State, Defense, the DNI, and NSA to review surveillance procedures and submit their findings to Congress.

H.R. 6304 rejects blanket immunity for telecommunications companies that may have participated in the administration's warrantless wiretapping program. Under this bill, lawsuits against these companies would be determined by Federal district courts. These telecommunications companies will have to prove that the Administration provided written assurance that their activities were legal. There is no immunity for any government official who may have violated the law included in this legislation.

This bill is much stronger than the Senate version, and will protect both our security and the civil liberties that we enjoy. I support the passage of H.R. 6304, FISA Amendments Act, and I urge my colleagues to vote in favor of this bipartisan measure as well.

Mr. LANGEVIN. Madam Speaker, I rise in support of the FISA Amendments Act of 2008. As a member of the Intelligence Committee, I know we must give our intelligence community the proper tools to protect us while upholding the civil liberties of Americans. Today's compromise illustrates what this House can do when it deliberates with care, holds steady against fear-mongering, and acts in the best interest of the country and its citizens.

This bill is strong on civil liberties, and includes protections against infringement of our Constitutional right to privacy.

First, the bill clarifies that FISA is the exclusive means by which the executive branch may conduct electronic surveillance on U.S. soil. No President will have the power to do an end-run around the legal requirements of FISA. This provision will prevent the types of abuses we have witnessed under this administration.

Second, this Act requires a warrant from the FISA court to conduct surveillance of Americans abroad. Americans will no longer leave their constitutional protections at home when working, studying, or traveling abroad.

Third, it requires prior approval by the FISA court of procedures the Government will use when carrying out foreign electronic surveillance. This will ensure that the Government's efforts are not aimed at targeting Americans, and that, if an American's communication is inadvertently intercepted, it is dealt with in a manner that guarantees legal protections.

One issue that has been repeatedly addressed is whether telecommunications companies should be granted immunity against pending lawsuits for their involvement in the earlier surveillance program. For a long period of time, the Bush Administration stonewalled and did not provide Congress the documents we demanded to ascertain the role that the telecommunications companies played. Since then, I have reviewed a large number of classified documents on this matter, and I am deeply concerned about the manner in which the Bush administration conducted its surveillance program. Therefore, I am pleased that this legislation preserves a role for the U.S. court system, which will review the documents produced by the White House and other relevant documents to decide independently whether the telecommunications companies acted in good faith when cooperating with the Government. Only after that review would the courts decide whether the telecommunications companies deserve any form of liability protection. Furthermore, the legislation authorizes a joint investigation by the Inspectors General from the U.S. Department of Justice, National Security Agency, Department of Defense, and Office of the Director of National Intelligence to review the past actions of the U.S. Government and report to Congress on their findings so that we may take appropriate action.

Many today have said that the legislation before us is not a perfect bill, and I agree. Nevertheless, it is significantly better than the bill passed by the Senate and an immense improvement over the Bush administration's program, neither of which took sufficient steps to protect Americans' civil liberties. I know that the Democratic leadership negotiated a good compromise, and I will support it. However, as I have said before, this legislation will only work if everyone involved follows the rules and remains within the confines of the law. Congress must continue to conduct robust oversight to make sure the law is implemented as intended to maintain the critical and fragile balance of protecting our Nation and protecting civil liberties.

Mr. LEVIN. Madam Speaker, I rise in opposition to the bill. I appreciate the hard work that Mr. HOYER and others have done on this legislation. The bill before the House is a vast improvement over the administration's Protect America Act, which I strongly opposed last August. The legislation is also a significant improvement over the seriously flawed FISA legislation approved by the Senate earlier this year. In many respects, the bill before the House strikes a reasonable balance between giving the Government the tools it needs to protect U.S. national security and protecting Americans' constitutional rights.

In particular, I am pleased that the bill reaffirms that the Foreign Intelligence Surveillance Act is the exclusive legal means by which the Government may conduct surveillance. This stands in stark contrast to the Bush administration's warrantless surveillance program. I also support the provisions of this bill that protect Americans traveling abroad. They need no longer leave their constitutional protections at home.

At the end of the day, I oppose this bill because of the provisions that would confer retroactive immunity on the telecommunications companies that participated in the Bush administration's warrantless surveillance program. We are a nation of laws, and it sets a dangerous precedent for Congress to approve a law that dismisses ongoing court cases simply on the basis that the companies can show that the administration told them that its warrantless surveillance program was legal. A program is not legal just because the administration claims that it is. The retroactive immunity provisions in this bill shield the administration from accountability for its actions. The goal here is not to harm the telecommunications carriers, but rather to get to the truth of what happened. A much better alternative would be to grant indemnification to the companies and go forward with the trials.

Irrespective of the outcome of today's vote, we need a full accounting of the administration's surveillance program, and the bill before the House provides for an Inspectors General audit describing all Federal programs involving warrantless surveillance conducted since September 11, 2001. The audit is to be completed within 1 year. Congress must get to the bottom of what happened and prevent it from happening again. It is essential that Congress follow up on the audit's findings with robust oversight.

Mr. DINGELL. Madam Speaker, while I cannot support the legislation before us today, I commend Majority Leader HOYER for the work he has done to negotiate a bill that is substantially better than the version that passed in the Senate. This legislation, which will be the exclusive mechanism for the Government to conduct surveillance within the United States,

contains provisions that will provide greater protections against unwarranted and unconstitutional searches of American citizens.

Despite the many improvements Mr. HOYER was able to obtain, I unfortunately still cannot support this legislation because it contains a provision that will grant immunity to the telecommunications companies that assisted the President with his illegal and unauthorized warrantless wiretapping program. I have consistently said that it is not appropriate for Congress to grant these companies immunity for their actions without having an understanding of what it is that they did. This is not only because it will hold the telecommunications companies accountable for their actions, but because it is the only way of finding out just how extensive the President's illegal wiretapping program really was. In other words, this provision will enable the Bush administration to continue suppressing facts and information about the Government's own misbehavior and wrongdoing.

The immunity provision contained in this bill purporting to allow for judicial review to determine whether immunity is appropriate is a sham. As drafted, courts will have no real discretion and will be forced to grant immunity so long as the Government claims its actions were legal. However, the court is under no obligation to investigate whether the Government's claims are true. Anyone following the headlines recently, who has read about the recent Supreme Court decision overturning the administration's argument that it has the authority to detain people indefinitely in Guantanamo Bay, or about the hearings held by Senator CARL LEVIN and the Senate Armed Services Committee uncovering evidence that top civilian leadership at the Department of Defense authored memos arguing it was legal for the military to torture detainees, should be extremely wary of trusting President Bush to decide whether or not it is legal to spy on Ameri-

Mr. HALL of New York. I have consistently supported modernizing the existing FISA law to give our Government the tools it needs to identify and defeat terrorists in today's hightech world, while at the same time preserving the freedoms and rights that define America. I have voted three times to pass legislation that would strengthen and modernize FISA and reaffirm the rule of law. Despite some improvements over previous attempts to update FISA. the bill considered by the House today regrettably falls short of achieving that critical balance. The rule of law lies at the core of America's founding principles, and the language in this bill was too weak to ensue that any breach of our laws that may have occurred under the warrantless wiretapping program will be fully addressed. It is not appropriate to deny Americans the right to pursue these matters in court, or to short-circuit the judicial review that lies at the heart of our system of checks and balances, which is the bedrock of our Constitution. Accordingly, I voted against this bill.

Mr. BLUMENAUER. Madam Speaker, I appreciate the hard work put in by my colleagues on both sides of the aisle and in both chambers. For the past year we've participated in substantial and sometimes heated debate on the issue of surveillance and foreign intelligence. I appreciate the good faith HOYER, as we try to craft legislation that keeps both our liberties and our persons safe.

For the past seven years I have been highly critical of Republican wiretapping legislation. I voted against past efforts to expand this administration's ability to intrude in the lives of unknowing and innocent Americans. I supported the expiration of the disgraceful Protect America Act. And I remain confident that the dedicated members of the intelligence community do not need to violate the rights of Americans in order to protect them.

I have heard some say that the enemies of America take on many forms. To them I say: Let us be sure one of those forms is not our own government.

Ultimately this is a compromise that falls short. Any gains in security that may be achieved are temporary and are more than outweighed by the longer-term loss of civil liberties and oversight. Although this bill is comparatively better than the Senate's version, I am troubled by the lack of robust government oversight, the absence of meaningful court review, and the risk to American liberties.

Of particular concern is the granting of de facto retroactive immunity to the telecommunications companies that cooperated with the administration. A 'doctor's note' from the Attorney General cannot be allowed to circumvent the entire judicial process.

I am equally concerned with the timeline of this bill, and strongly oppose authorizing this legislation for four years. This will extend the Bush legacy throughout the next administration and the next two sessions of Congress. Frankly I see no reason to rush into a compromise that comes up this short. The American people would be better served if we continued to debate this issue and took up a bill after we have seen the last of this administration. Americans demand and deserve protection of their basic civil rights and this can be accomplished while providing the means necessary for our intelligence community to do its inch.

Mr. NADLER. Madam Speaker, Members of the House must decide today whether to uphold the rule of low and the supremacy of the Constitution or whether to protect and reward the lawless behavior of the administration and of the telecommunications companies that participated in its clearly illegal program of spying on innocent Americans.

This bill limits the courts hearing lawsuits alleging illegal wiretapping to consider only whether the telecom companies received a "written request or directive . . . indicating that the activity was [] authorized by the President; and [] determined to be lawful"—not whether the request was actually lawful or whether the telecom companies knew that it was unlawful.

The bill is a fig-leaf, granting blanket immunity to the telecom companies for illegal acts without allowing the courts to consider the facts or the law. It denies people whose rights were violated their fair day in court, and it denies the American people their right to have the actions of the administration subjected to fair and independent scrutiny.

Even the courts' limited review will remain secret. The lawsuits will be dismissed, but the basis for the dismissal—that the defendants were innocent of misconduct, or that they were guilty but Congress commands their immunity—must remain secret.

And the constitutionality of the immunity granted by this bill is very questionable. As Judge Walker put it in the AT&T case:

AT&T's alleged actions here violate the constitutional rights clearly established in [the] Keith decision. Moreover, because 'the very action in question has previously been held unlawful,' AT&T cannot seriously contend that a reasonable entity in its position could have believed that the alleged domestic dragnet was legal.

I would hope that the courts will find that, because the Constitutional rights of Americans have been violated, Congress' attempt to prevent court review is unconstitutional.

The bill also reiterates than FISA and specified other statutes are the exclusive legal authority for electronic surveillance. The Act has always said that. This bill adds some new mechanisms to ensure that any future legislation may not be read to override this exclusivity by implication, but only by explicitly saying that that is its purpose.

No one and no court should draw the false conclusion that we are thereby implying that the exclusivity provision was, or could have been, overridden either by the President's claim of inherent authority under Article II of the Constitution, or by the Authorization for the Use of Military Force of 2001. This bill does not say or imply that. If there is any doubt of this point, the blanket immunity provisions of this bill reflect Congress' understanding that this domestic spying was not legal. If it were, there would not be any necessity for these provisions.

This bill abandons the Constitution's protections and insulates lawless behavior from legal scrutiny.

I urge a "no" vote.

Mr. BOSWELL. Madam Speaker, I rise in support of H.R. 6304.

This is the kind of work I came to Congress hoping for—bipartisan legislation that protects our security and our liberty. It's a solid compromise that does what it needs to do for the country.

One of my specific concerns in FISA reform over the last year has been finding a way to protect reasonable private companies, who assisted government out of patriotism.

This bill does that. It doesn't give anyone a free pass, but it allows companies to come before the courts and make their case in order to be protected from lawsuits.

That's a good result, and I thank Chairman REYES for his work in reaching this reasonable bipartisan compromise.

I urge my colleagues to vote "yes."

Ms. GINNY BROWN-WAITÉ of Florida. Madam Speaker, I rise today in support of H.R. 6304, a bill to reauthorize the Foreign Intelligence Surveillance Act and to protect America from foreign threats.

For the past several months, I have heard from hundreds of constituents on the issue of FISA.

Each one of them expressed their alarm and disbelief that the House Majority would repeatedly refuse to call a vote on bipartisan legislation to extend FISA and address our grave vulnerability to terrorist attacks.

Today I am pleased that the Majority leadership has finally reached across the aisle to put together a compromise bill, and fulfill one of its fundamental tasks—to ensure the security of this great Nation.

This compromise is also a reminder of what I have always believed, that no one side can do it alone; both parties must work together to ensure our safety.

In such uncertain times, when it is essential that our government utilize every available tool to protect American citizens, having the ability to collect intelligence responsibly is essential.

While there is no excuse for the delay in bringing this critical bill to the floor, we must now move forward together to pass H.R. 6304 and restore our Nation's intelligence capabilities.

Mr. REYES. Madam Speaker, I yield back the remainder of our time.

The SPEAKER pro tempore. All time for debate has expired.

Pursuant to House Resolution 1285, the bill is considered read and the previous question is ordered.

The question is on the engrossment and third reading of the bill.

The bill was ordered to be engrossed and read a third time, and was read the third time.

The SPEAKER pro tempore. The question is on the passage of the bill.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. CONYERS. Madam Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The vote was taken by electronic device, and there were—yeas 293, nays 129, not voting 13, as follows:

[Roll No. 437]

YEAS-293

Green, Gene

Gutierrez

Cleaver

Clyburn

Ackerman

Aderholt

Akin Coble Hall (TX) Cole (OK) Alexander Harman Hastings (FL) Altmire Conaway Arcuri Cooper Hastings (WA) Baca Costa Haves Bachmann Cramer Heller Bachus Crenshaw Hensarling Baird Crowley Herger Barrett (SC) Herseth Sandlin Barrow Cuellar Higgins Bartlett (MD) Culberson Hinojosa Barton (TX) Davis (AL) Hobson Rean Davis (KY) Hoekstra Berkley Davis, David Holden Berman Davis, Lincoln Berry Davis Tom Hulshof Deal (GA) Biggert Hunter Inglis (SC) Bilbray Dent Diaz-Balart, L. **Bilirakis** Tssa. Bishop (GA) Diaz-Balart, M. Johnson, Sam Bishop (NY) Dicks Jordan Bishop (UT) Donnelly Kanjorski Blackburn Doolittle Keller Blunt Drake Kildee Boehner Dreier Kind Bonner Duncan King (IA) Edwards (TX) Bono Mack King (NY) Ehlers Boozman Kingston Ellsworth Boren Kirk Boswell 8 | Emanuel Klein (FL) Boucher Emerson Kline (MN) Boustany Engel Knollenberg English (PA) Boyd (FL) Kuhl (NY) Boyda (KS) Etheridge LaHood Lamborn Brady (TX) Everett Broun (GA) Fallin Lampson Brown (SC) Feeney Langevin Brown, Corrine Ferguson Latham Buchanan Flake LaTourette Latta Burgess Forbes Burton (IN) Fortenberry Lewis (CA) Butterfield Fossella Lewis (KY) Foxx Linder Buyer Calvert Franks (AZ) Lipinski Camp (MI) Frelinghuysen LoBiondo Campbell (CA) Gallegly Lowey Garrett (NJ) Cantor Lucas Lungren, Daniel Capito Gerlach Cardoza Giffords E. Carney Gillibrand Mack Mahoney (FL) Carter Gingrey Castle Goode Manzullo Castor Goodlatte Marchant Cazayoux Gordon Marshall Chabot Granger Matheson McCarthy (CA) Chandler Graves Green, Al McCarthy (NY) Childers

Pryce (OH) McCaul (TX) Skelton McCotter Putnam Smith (NE) Smith (NJ) McCrery Radanovich McHenry Rahall Smith (TX) Ramstad McHugh Smith (WA) McIntyre Regula Snyder McKeon Rehberg Souder McMorris Reichert Space Rodgers Renzi Spratt McNerney Reves Stearns Meeks (NY) Richardson Stunak Melancon Rodriguez Sullivan Mica. Rogers (AL) Tancredo Miller (FL) Rogers (KY) Tanner Miller (MI) Rogers (MI) Tauscher Miller, Gary Rohrabacher Mitchell Ros-Lehtinen Taylor Moore (KS) Roskam Terry Thompson (MS) Moran (KS) Ross Murphy, Patrick Royce Thornberry Ruppersberger Murphy, Tim Tiberi Ryan (WI) Murtha Turner Salazar Musgrave Udall (CO) Myrick Sali Upton Neugebauer Saxton Walberg Scalise Walden (OR) Ortiz Schiff Walsh (NY) Schmidt Pearce Wamp Pelosi Scott (GA) Weldon (FL) Pence Sensenbrenner Westmoreland Perlmutter Sessions Whitfield (KY) Peterson (MN) Sestak Wilson (NM) Shadegg Petri Wilson (OH) Pickering Shays Wilson (SC) Pitts Sherman Wittman (VA) Platts Shimkus Wolf Poe Shuler Yarmuth Pomeroy Shuster Young (AK) Porter Simpson Price (GA) Sires Young (FL)

NAYS-129

Abercrombie Holt Oberstar Honda Allen Obey Andrews Hooley Olver Baldwin Pallone Inslee Becerra IsraelPascrell Jackson (IL) Blumenauer Pastor Brady (PA) Jackson-Lee Payne Braley (IA) (TX) Price (NC) Capps Jefferson Rangel Rothman Johnson (GA) Capuano Carnahan Johnson (IL) Roybal-Allard Johnson, E. B. Ryan (OH) Sánchez, Linda Carson Clarke Jones (OH) Kagen Clay Т. Cohen Sanchez Loretta Kaptur Kennedy Sarbanes Conyers Costello Kilpatrick Schakowsky Courtney Kucinich Schwartz Scott (VA) Larsen (WA) Cummings Davis (CA) Larson (CT) Serrano Davis (IL) Shea-Porter Lee DeFazio Levin Slaughter DeGette Lewis (GA) Solis Delahunt Loebsack Speier DeLauro Lofgren, Zoe Sutton Dingell Lynch Thompson (CA) Malonev (NY) Doggett Tiernev Markey Doyle Towns Edwards (MD) Matsui Tsongas Udall (NM) Ellison McCollum (MN) Eshoo McDermott Van Hollen Farr McGovern Velázquez Fattah Walz (MN) McNultv Filner Meek (FL) Wasserman Foster Michaud Schultz Frank (MA) Miller (NC) Waters Gonzalez Miller, George Watson Grijalya. Mollohan Watt Hall (NY) Moore (WI) Waxman Hare Moran (VA) Weiner Welch (VT) Hill Murphy (CT) Hinchey Nadler Wexler Napolitano Hirono Woolsey

NOT VOTING—13

Wu

Brown-Waite, Jones (NC) Stark
Ginny Paul Tiahrt
Cannon Peterson (PA) Visclosky
Gilchrest Reynolds Weller
Gohmert Rush

Neal (MA)

Hodes

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore (during the vote). There are 2 minutes remaining in this vote.

□ 1248

Mr. FRANK of Massachusetts, Mr. JEFFERSON, Mrs. CAPPS and Ms. KAPTUR changed their vote from "yea" to "nay."

Mr. BERMAN changed his vote from "nay" to "yea."

So the bill was passed.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

Stated against:

Mr. VISCLOSKY. Madam Speaker, had I been present for rollcall 437, H.R. 6304, on passage of a measure to amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes, I would have voted "nay."

REMOVAL OF NAME OF MEMBER AS COSPONSOR OF H.R. 3192

Ms. ZOE LOFGREN of California. Mr. Speaker, I ask unanimous consent that my name be removed as a cosponsor of H.R. 3192.

The SPEAKER pro tempore (Mr. ARCURI). Is there objection to the request of the gentlewoman from California?

There was no objection.

REMOVAL OF NAME OF MEMBER AS COSPONSOR OF H.R. 6041

Mr. BRADY of Texas. Mr. Speaker, I seek unanimous consent to remove my name as a cosponsor of H.R. 6041.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Texas?

There was no objection.

LEGISLATIVE PROGRAM

(Mr. BLUNT asked and was given permission to address the House for 1 minute.)

Mr. BLUNT. Mr. Speaker, I yield to my good friend from Maryland, the majority leader, for information about next week's schedule.

Mr. HOYER. I thank the Republican whip for yielding.

On Monday, the House will meet at 12:30 p.m. for morning hour and 2 p.m. for legislative business with votes postponed until 6:30 p.m.

On Tuesday, Mr. Speaker, the House will meet at 9 a.m. for morning hour and 10 a.m. for legislative business.

Mr. Speaker, we will consider several bills under suspension of the rules, including a bill to address cuts in Medicare physician rates. I will reiterate that. We will have a suspension bill on Medicare physician rates.

The complete list of suspension bills will be announced by the close of business today.